RUHR-UNIVERSITÄT BOCHUM

RUB

isits
International School
of IT Security AG

Consumerisation und BYOD

Konzeption und Erstellung eines IT-Grundschutz-Bausteins

Masterarbeit im Studiengang „Applied IT Security“ (AITS)
Fakultät für Elektrotechnik und Informationstechnik

Autor: XXX
Matr. Nr. XXX
xxx@xxx.xx

Betreuer: XXX XXX
xxx@xxx.xx

1. Prüfer: XXX XXX

2. Prüfer: XXX XXX

Abgabe: 07. Mai 2019

Zusammenfassung

Zielsetzung dieser Masterarbeit ist die Betrachtung des Themas *Consumerisation und Bring your own Device (BYOD)* zur Konzeption und Erstellung eines Bausteins für das IT-Grundschutz-Kompendium des Bundesamt für Sicherheit in der Informationstechnik (BSI). Nach Einführung zu den Themen *Consumerisation und BYOD* und dem *IT-Grundschutz*, werden Strategien zur Einbindung von mobilen Geräten im institutionellen Umfeld untersucht. Die Ergebnisse fließen in die Konzeption und anschließende Erstellung des IT-Grundschutz Bausteins mit ein. Abschließend wird eine Implementierung der Arbeitsergebnisse in Form einer Abfrage mit Anwendern aus der Praxis getestet und zur Optimierung des Bausteins eingesetzt. Der resultierende Baustein liegt danach als interner Arbeitsentwurf vor und soll, entsprechend dem Veröffentlichungsworkflow des BSI, später bis in die finale Version (Edition) weiterentwickelt und veröffentlicht werden.

The objective of this master thesis is to consider the topic of consumerization and bring your own device (BYOD) for the conception and creation of a component for the IT-basic protection Compendium of the Federal Office for Security in information technology (BSI). Following the introduction to the topics of consumerization and BYOD plus IT basic protection, strategies for the integration of mobile devices in the institutional environment will be examined. The results will be incorporated in the conception and subsequent creation of the IT basic protection component. Finally, the results of the work will be tested and implemented in interviews with actual users in order to optimize the module. The resulting module will then be available as an internal draft. It will be continually developed in accordance to the publication workflow of the BSI, until the final version (Edition) has been completed and will then be published.

Eidesstattliche Erklärung

Ich erkläre, dass ich keine Arbeit in gleicher oder ähnlicher Fassung bereits für eine andere Prüfung an der Ruhr-Universität Bochum oder einer anderen Hochschule eingereicht habe. Ich versichere, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Die Stellen, die anderen Quellen dem Wortlaut oder dem Sinn nach entnommen sind, habe ich unter Angabe der Quellen kenntlich gemacht. Dies gilt sinngemäß auch für verwendete Zeichnungen, Skizzen, bildliche Darstellungen und dergleichen. Ich versichere auch, dass die von mir eingereichte schriftliche Version mit der digitalen Version übereinstimmt. Ich erkläre mich damit einverstanden, dass die digitale Version dieser Arbeit zwecks Plagiatsprüfung verwendet wird.

Datum	XXX

Erklärung

Ich erkläre mich damit einverstanden, dass meine Masterarbeit am Lehrstuhl dauerhaft in elektronischer und gedruckter Form aufbewahrt wird und dass die Ergebnisse aus dieser Arbeit unter Einhaltung guter wissenschaftlicher Praxis in der Forschung weiter verwendet werden dürfen.
Zusätzlich räume ich hiermit (von meiner Seite aus) dem BSI die Nutzungsrechte an den Ergebnissen dieser Arbeit ein.

Datum	XXX

Inhaltsverzeichnis

1 Einleitung

Die zunehmende Integration mobiler Geräte in den Alltag, hat auch Einfluss auf die berufliche Arbeitsweise. Der Wunsch der Arbeitnehmer, außerhalb der Institution auf Geschäftsdaten zugreifen zu können, führt zu einem Aufbruch der informationstechnischen Grenzen, was die Komplexität der Informationssicherheitsstruktur erhöht. Die Begriffe *Consumerisation und BYOD* beschreiben diese Strategie. Dieser Bedarf stellt die Institution vor neue Herausforderungen, die zugleich Chancen und Risiken bergen.
Standardisierte Vorgehensweisen für Institutionen um solche und ähnliche Probleme der Informationssicherheit zu handhaben, stellt das BSI in Form des IT-Grundschutz zur Verfügung.

1.1 Zielsetzung

Durch die vielen möglichen Szenarien und Einflüsse auf die Akteure, scheint es Ad-Hoc eine schwierige Aufgabe allgemein gültige Sicherheitsstrategien zum Thema *Consumerisation und BYOD* zu entwickeln. Informationssicherheitsbeauftragte einer Institution, die durch *Consumerisation und BYOD* nun mit eben diesen komplexeren Anforderungen konfrontiert werden, sollen auch in dieser Fragestellung durch den IT-Grundschutz eine strukturierte Hilfestellung erhalten. Die Untersuchung dieser wichtigen Thematik und die Konzeption und Erstellung des passenden IT-Grundschutz-Bausteins auf dieser Basis ist die Motivation zu dieser Arbeit.

1.2 Der IT-Grundschutz

Der IT-Grundschutz ist ein vom BSI entwickeltes systematisches Vorgehen, notwendige Sicherheitsmaßnahmen für Institutionen zu identifizieren und umzusetzen. Er dient dazu, „das Niveau der Informationssicherheit in Behörden und Unternehmen

jeder Größenordnung zu erhöhen“.[1] Den IT-Grundschutz gibt es bereits seit ca. 1994 bzw. 1995. Nach kleineren Aktualisierungen und Modifikationen, wurde die IT-Grundschutz-Methodik im Herbst 2017 einer grundlegenden Modernisierung unterzogen. Die Inhalte wurden stärker fokussiert und verschlankt sowie neue Themen und Aspekte integriert.
Der Aufbau ist in zwei Säulen unterteilt: Die BSI-Standards und das IT-Grundschutz-Kompendium. Die Methoden und Vorgehensweisen sind in den BSI-Standards 200-1 (Anforderungen an ein Managementsystem für Informationssicherheit (ISMS))[9], 200-2 (IT-Grundschutz-Methodik)[10] und 200-3 (Risikomanagement)[11] veröffentlicht. Im IT-Grundschutz-Kompendium[13] sind die Bausteine, die jeweils Gefährdungen und Anforderungen für ein Thema der Informationssicherheit enthalten. Sie sind in Prozess- und System-Bausteine aufgeteilt und in insgesamt zehn Schichten untergliedert. Zusätzlich werden vereinzelt Umsetzungshinweise mit Maßnahmen für verschiedene Schutzbedarfsstufen (Basis, Standard und erhöhter Schutzbedarf) angeboten. Seit 2018 erscheint das IT-Grundschutz-Kompendium jährlich in einer aktualisierten Auflage.
Aktuell existiert im novellierten IT-Grundschutz noch keine explizite Berücksichtigung des Themas *Consumerisation und BYOD* in einem eigenen Baustein. Lediglich Teilaspekte sind in Bausteinen anderer Themengebiete berücksichtigt. Der zunehmende Bedarf und die damit einhergehenden neuen Anforderungen (z.B. Erweiterung des Informationsverbundes, Trennung privater und institutioneller Informationen), könnte bedrohlich für die Informationssicherheitslage der verbundenen Institution sein. Deshalb erscheint es sinnvoll, den Umgang mit dieser Thematik konzentriert in einem eigenen Baustein abzubilden.

[1] `https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/itgrundschutzAbout_node.html`

2 Consumerisation und BYOD

Dieses Kapitel dient zur Einordnung der Begrifflichkeiten (Kap. 2.1) und zur Vorstellung einiger gängigen, zur erfolgreichen Umsetzung zugrunde liegenden, Technologien (Kap. 2.3). Abschließend werden anhand einiger Institutionen derzeit gängige Strategien bezüglich *Consumerisation und BYOD* dargestellt (Kap. 2.4).

2.1 Definition und Abgrenzung

Im Kern stehen die Begriffe *Consumerisation* und *Bring your own Device* beide für die kombinierte geschäftliche und private Nutzung eines (mobilen) Gerätes. *Consumerisation* wird in Analogie zu *Bring your own Device (BYOD)* oft auch als *Choose your own Device (CYOD)* bezeichnet und umfasst Geräte, die durch die Institution ausgewählt und zur Verfügung gestellt werden. Im Gegensatz dazu sind die Geräte bei *BYOD* privates (ggf. durch die Institution subventioniertes) Eigentum des Mitarbeiters, der dieses dann auch geschäftlich nutzen kann. Die grundlegenden Unterschiede werden nochmals in Tabelle 2.1 aufgelistet.

Tabelle 2.1: Unterschiede zwischen Consumerisation und Bring your own Device (BYOD)

Begriff	**Consumerisation**	**Bring your own Device**
Geräteauswahl	Institution	Mitarbeiter
Gerätebesitz	Institution	Mitarbeiter[a]
Komplexität	Mittel	Hoch

[a] ggf. durch Institution subventioniert

Consumerisation ist eine vereinfachte Variante von *BYOD*. Während viele Aspekte (mobile private/berufliche Nutzung) gleich sind, so wird durch die Vorauswahl und Bereitstellung möglicher Geräte die Komplexität im Betrieb gesenkt. Zur Vereinfachung des Vorgehens wird deshalb im weiteren Verlauf der Arbeit nur noch der Begriff *BYOD* verwendet.

2.1.1 Ausprägungen

Hinsichtlich BYOD werden nach Monsch unterschiedliche Ausprägungen unterschieden [vgl. 35, S.24 f.]:

- **Als Betriebsmittelersatz**: Private Endgeräte werden (vertraglich fixiert) vollständig zur Arbeitserfüllung eingesetzt.
- **Optionaler Einsatz**: Möglichkeit ein privates Endgerät zusätzlich mit in die Arbeitsorganisation einzubringen und zu verwenden. Betriebliche Geräte müssen weiterhin angeboten werden.
- **Nicht geregelter Einsatz**: Nutzung privater Endgeräte wird zwar geduldet, es existieren jedoch keine verbindliche Nutzungsregelungen und Rahmenbedingungen. Wird auch als *BYOD-Wildwuchs* bezeichnet und sollte aus sicherheitstechnischer Sicht vermieden werden.

Sowohl zur Realisierung der Szenarien **als Betriebsmittelersatz** als auch **optionaler Einsatz** wird seitens der Institution eine gründliche Planung und Einführung benötigt.

2.1.2 Pro und Contra

Zur Entscheidungsfindung ob eine Einführung von BYOD sinnvoll ist, stellt sich schnell die Frage: *„Was spricht für und was gegen BYOD?“*
In einem Report von Hayes und Kotwica werden auf diese Frage folgende Vor- und Nachteile [vgl. 22, S.2] genannt:

Vorteile

- Verbesserte Benutzererfahrung durch Vertrautheit und Reduktion auf nur ein Gerät
- Möglichkeit zum Transfer der Hardwarekosten vom Unternehmen auf den Mitarbeiter
- Verbesserte Arbeitsmöglichkeiten ohne Rücksicht auf Zeit und Ort
- Verbesserung der Kreativität durch freie Wahl der Arbeitsumgebung („Best Places to Work“)
- Verbesserung der Produktivität

Nachteile

- Gefahr des Entscheidungsverlusts der Firma hinsichtlich der Bündelung von Hardware, Software und Nutzung

- Erhöhte Komplexität des firmeneigenen IT-Supports aufgrund unterschiedlicher Plattformen und Geräten
- Mögliche Kompatibilitätsprobleme von Hard- und Software mit der firmeneigenen Software und IT-Infrastruktur
- Grenzen zwischen persönlichen und beruflichen Informationen verschwimmen
- Einführung neuer Sicherheits- und Datenschutzrichtlinien beschränken Möglichkeiten

Vor- und Nachteile zugleich

- Notwendigkeit zur regelmäßigen Aktualisierung der Hardware mit aktuellen Funktionalitäten

Hayes und Kotwica nennen in ihrer Auflistung der Vorteile vor allem Argumente, die die gesteigerte Effizienz und Flexibilität durch BYOD betonen. Die Nachteile sehen sie vor allem aus Sicht der Institution und zudem mit Schwerpunkt auf technische Aspekte.

Einen weiteren ergänzenden Aspekt nennt ein Team der George Washington University um Zahadat et al. in ihrer Untersuchung. Sie stellen die These auf, dass Mitarbeiter dazu tendieren ihre eigenen Geräte sorgfältiger zu behandeln als wenn diese der Institution gehören würden [vgl. 51, S.82]. Es werden keine pauschalen Nachteile genannt, jedoch bereits konkrete Probleme [vgl. 51, S.83], die im Zusammenhang mit einem nicht ausreichend geregeltem BYOD-Einsatz auftreten können:

- **Inkonsistente Sicherheitsrichtlinien:** Können beispielsweise dazu führen, dass auf Desktops komplexe Passwörter gesetzt werden müssen, während auf BYO-Geräten auch ein 4-stelliger PIN-Code toleriert wird.
- **Datenverbreitung durch geteilte Medien:** Wenn Verschlüsselung nicht gefordert wird, können beispielsweise durch Datenaustausch auf externen Speichern, sensitive Daten unkontrolliert in die Öffentlichkeit gelangen.
- **Minimalistisches Gerätemanagement:** BYO-Geräte erlangen oftmals sehr unreglementierten Zugriff auf das Institutions-Netzwerk und können dort Dienste nutzen.
- **Lesbare Daten verbleiben auf ausgesonderten Geräten:** Vielfach enthalten aussortierte oder verkaufte Geräte noch sensitive Informationen, die auch trotz Löschung noch rekonstruiert werden können.

- **Datenaustausch zwischen Apps:** Wenn Informationen auf BYO-Geräte geladen werden, kann standardmäßig nicht sichergestellt werden, dass diese nur in den Apps verbleiben, für die sie auch bestimmt waren. Durch Sync-Tools können Informationen zudem in Clouds geladen oder in ungeeignete Backups gesichert werden.

Diese Auflistung einiger möglicher Schwierigkeiten, illustriert bereits recht gut, auf wie vielen unterschiedlichen Ebenen der BYOD-Einsatz Probleme verursachen kann.

Es lässt sich feststellen, dass es gewichtige Pros aber auch Contras gibt und immer im Einzelfall entschieden werden muss, ob der Einsatz von BYOD für bestimmte Szenarien sinnvoll ist. Einige der genannten Nachteile lassen sich durch entsprechende Maßnahmen abmildern oder gar vermeiden. Trotzdem muss vor allem zunächst die Institution entscheiden, ob für sie die Vorteile überwiegen und sie BYOD realisieren möchte. Zahadat et al. geben in diesem Zusammenhang jedoch zu bedenken: „Organizations sometimes start out by saying 'no' to BYOD only to find out later they have been participants through email, text messages, and document sharing.“ [51, S.83] Zu viel Restriktion kann folglich also auch schnell das Gegenteil bewirken und eine Unterwanderung der Compliance durch die Mitarbeiter zur Folge haben.
Einen Schlüsselfaktor zur Vermeidung von Sicherheitsproblemen sehen Zahadat et al. darin, das die Institution den Mitarbeiter zu einem Teil ihres Sicherheitskonzepts machen sollte: „Since in a BYOD environment, the organization does not own the desktop (devices are privately owned and are portable), the solution to their security concerns seems to be to make the user part of their security model...“ [51, S.83]
In diesem Zusammenhang sollte auch die Motivation des Mitarbeiters zur Nutzung von BYOD beachtet werden. Hovav und Putri haben festgestellt, dass die wahrgenommene Verbesserung der Effizienz und eine empfundene Gerechtigkeit hinsichtlich der Richtlinien, Mitarbeiter eher die BYOD-Ausrichtung der Institution akzeptieren lässt. Negativ fassen diese die damit zusammenhängende wahrgenommene Einschränkung ihrer Freiheit auf, wenn die Institution ihre Richtlinien bzgl. BYOD anwendet [vgl. 25, S.35]. Ein Beispiel dazu: „The requirements of a strong password may slow down the access time to the device.“[25, S.35] Diese umfangreiche Untersuchung belegt, dass der Erfolg eines BYOD-Programms auch im großen Maße vom Gleichgewicht der BYOD-Richtlinien zwischen dem Schutz der institutionellen Informationen einerseits und der größtmöglichen Freiheit des BYOD-Nutzers auf der anderen Seite abhängt.

2.1.3 Lifecycle

Zur Verdeutlichung in welchem Umfang BYO-Geräte in der Planung zu berücksichtigen sind, hilft die Betrachtung eines BYOD-Lifecycles. Nach Zahadat et al. geschieht

dies, wie in Abb.2.2 dargestellt, in vier Phasen. [51, S.84]

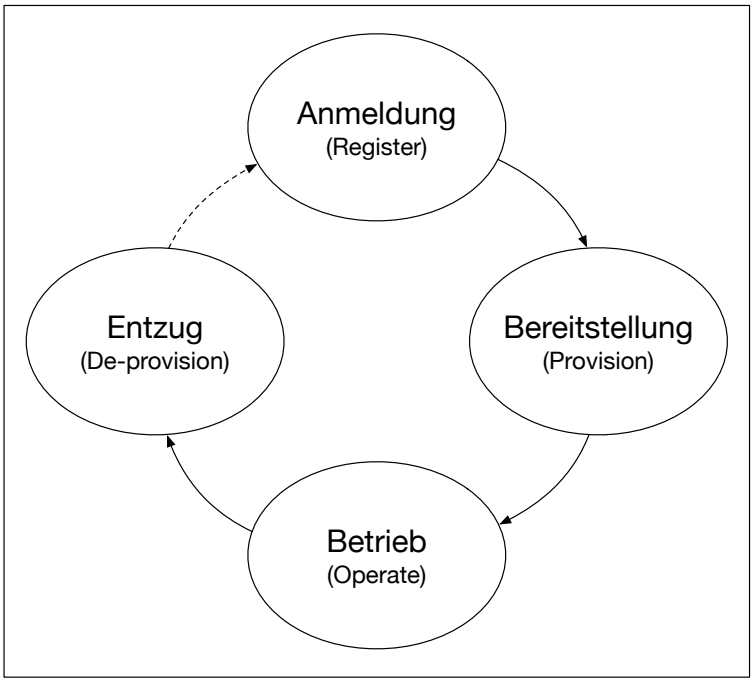

Abbildung 2.2: Basis BYOD-Lifecycle

1. **Register:** Überprüfung, ob das Gerät die grundsätzlichen Voraussetzungen zur Teilnahme am BYOD-Programm erfüllt
2. **Provision:** Einbindung des Gerätes durch eine (automatisierte) Installation von Konfigurationen, Einstellungen, Applikationen und Zertifikaten, die für den sicheren Betrieb benötigt werden.
3. **Operate:** Der Benutzer erhält im Rahmen von BYOD Zugriff auf institutionelle Informationen und Dienste.
4. **De-provision:** Das Gerät soll nicht länger am BYOD-Programm teilnehmen. Entfernung aller institutionellen Informationen, Einstellungen, Zertifikate und Einschränkungen.

Gerade die Inhalte der letzten Phase, das *De-provision*, werden im ungeregelten Zustand schnell vernachlässigt und können die Informationssicherheit der Institution gefährden.

Die Betrachtung eines detaillierteren Lifecycles mit acht Schritten, wie in Abb.2.3 dargestellt, empfehlen Kohne et al. [27, S.102].

Nach Auffassung von Kohne et al. ähnelt dieser Lifecycle grundlegend dem Prozess wie er auch für normale IT-Systeme stattfindet. „Die Reihenfolge ändert sich aber

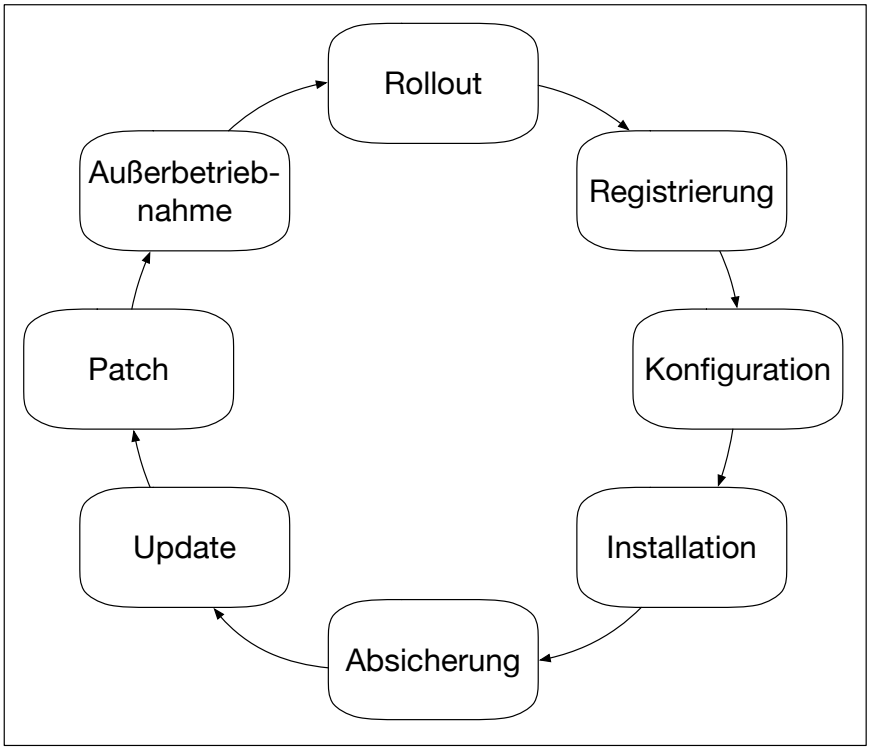

Abbildung 2.3: BYOD-Lifecycle

in Teilen, da die Geräte von den Mitarbeitern dezentral beschafft, konfiguriert und betrieben werden.“ [27, S.102]

Folgende Schritte werden durchlaufen:

- **Rollout:** Anschaffung und Übergabe an den Nutzer durch die Institution oder durch den Mitarbeiter. Von nun an kann dieser das Gerät grundsätzlich einsetzen.
- **Registrierung:** Erstregistrierung um bestimmte Funktionen zu nutzen. Nach Kohne et al. muss hier zwischen Registrierungen beim Diensteanbieter bzw. Hersteller (Aktivierung) und in der Management-Lösung zum Zugriff auf Daten und Dienst der Institution unterschieden werden.
- **Konfiguration:** Einstellen der benötigten Sicherheitseinstellungen.
- **Installation:** Einrichtung von Applikationen auf dem Gerät. Der Benutzer sollte nach Sicht von Kohne et al. jederzeit beliebige Software installieren können. Eine Einschränkung kann in Form von Black- oder Whitelists erfolgen oder kann sogar bei Wahl einer Container-Lösung vermieden werden. Mittels Management-Lösung können auch eine App-Auswahl automatisiert installiert oder über einen Enterprise App Store angeboten werden.

- **Absicherung:** Sicherung und Trennung privater und geschäftlicher Daten durch Verschlüsselung der Informationen auf dem Gerät sowie Nutzung verschlüsselter Kommunikationswege für schützenswerte Daten.

- **Update:** Betriebssystem-Aktualisierungen (Hersteller) und Updates können automatisiert installiert werden. Kohne et al. empfehlen die Aktvierung automatisierter Updates über die Management-Plattform.

- **Patch:** Neben den Updates differenzieren Kohne et al. so genannte Patches in einem gesonderten Schritt als Programme, „die zum Beispiel Sicherheitslücken in Betriebssystemen und Apps schließen." [27, S.107] und empfehlen eine umgehende Installation.

- **Außerbetriebname:** Bei Außerbetriebsetzung eines Gerätes müssen zuvor alle privaten und institutionellen Daten gesichert und danach alle wichtigen Apps, Daten, Netzzugänge, Zertifikaten und Konfigurationen mit Hilfe der Management-Software gelöscht werden. Nach Kohne et al. gilt es noch zu unterschieden, ob lediglich ein Gerätetausch stattfinden soll oder ob es sich um einen Verlust/Diebstahl handelt, bei dem deutlich schneller reagiert werden muss.

Beide vorgestellten Lifecycle-Modelle zeigen, dass ein BYO-Gerät von der Anschaffung bis zur Aussonderung kontinuierliche Aufmerksamkeit in unterschiedlichen Disziplinen benötigt. Wenn dieser Prozess einmal in Gang gesetzt wird, sollte die Institution bereits die notwendigen Tätigkeiten auf allen Stufen geplant haben. Vor einer voreiligen BYOD-Umsetzung warnen auch Zahadat et al.: „On the other hand, many organizations embrace it rapidly and then are overwhelmed by the security and privacy implications." [51, S.83] Folglich ist eine umfassende Planung für eine erfolgreiche BYOD-Initiierung unerlässlich.

2.2 Umsetzung in die Praxis

Anhand des in Kapitel 2.1.3 dargestellten BYOD-Lifecycles (Abb.2.3) sollen in diesem Kapitel kurz die Aspekte zur erfolgreichen Einführung und einem nachhaltigen Betrieb untersucht werden. Dazu bedarf es zunächst einer gut geplanten Vorbereitung. Aber auch im Betrieb gibt es noch eine Reihe von Aufgaben, die für eine nachhaltige Etablierung von BYOD in der Institution von Nöten sind.

2.2.1 Vorbereitung des Unternehmens

Der Umfang der Realisierung von BYOD in der Institution ist zunächst eine Frage des Risikoappetits, der vor allem von der jeweiligen Branche bestimmt wird. Beispielsweise ist von Institutionen der Finanzbranche eine eher defensive Haltung zu erwarten. Die Einordnung bestimmt unter anderem die Restriktionen hinsichtlich der Geräteauswahl, den Richtlinien, den Funktionen und des Supports. [vgl. 34, S.3] Das Schaubild aus Abb.2.4 illustriert diese Zuordnung.

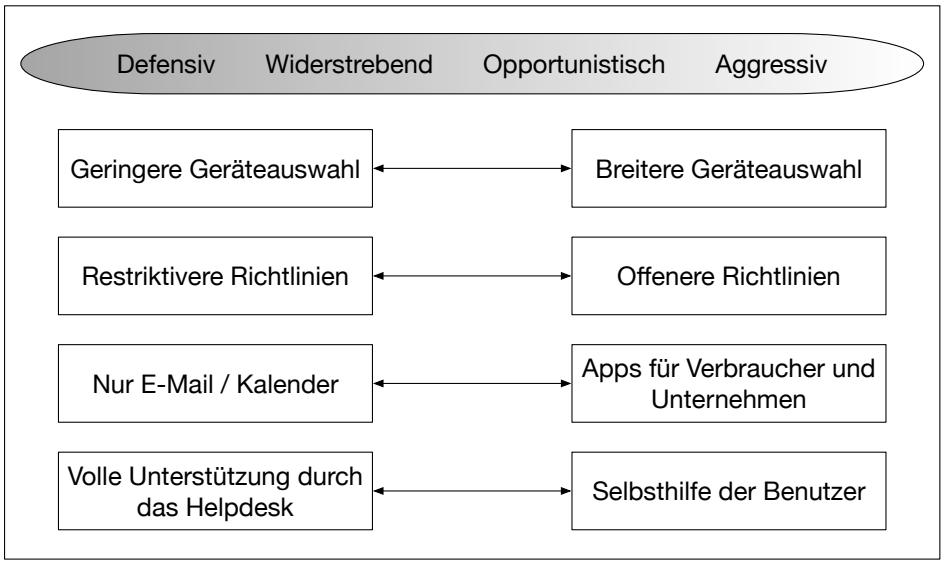

Abbildung 2.4: Risikoappetit und Auswirkungen auf das BYOD-Programm

Zahadat et al. schließt sich dieser Einschätzung an: „Creating a security program requires insight into the risk appetite of the organization along with hundreds of decisions to be made by senior leadership . . . .“ [51, S.85] Weiter fordern Zahadat et al. an dieser Stelle die Einbindung aller Entscheidungsträger und die Unterstützung durch die höchste Management-Stufe um die notwendigen Ressourcen zur Verfügung zu haben [vgl. 51, S.85 ff.].

Auch MobileIron empfiehlt in seinem BYOD-Guide frühzeitig betroffene Interessengruppen in die Planung mit einzubeziehen.

Ein BYOD-Lenkungsausschuss, bestehend aus Vertretern dieser Gruppen, kann Bedenken gleich zu Beginn aufnehmen und im Idealfall zerstreuen. Eine mögliche Aufgabe für diesen Ausschuss wäre beispielsweise auch die Klärung einiger Rahmenbedingungen. Folgende Aspekte könnten nach Hayes und Kotwica an dieser Stelle unter anderem zur Diskussion stehen [vgl. 22, S.2 f.]:

- Definition der Gültigkeit: Personen, Geräte, Daten, Applikationen

- Wer trägt die Kosten und in welcher Weise? Arbeitnehmer oder Arbeitgeber? Volle oder teilweise Kostenübernahme?
- Wer bietet Produktunterstützung? Institution, Arbeitnehmer oder Geräteanbieter?
- Verantwortlichkeiten des Benutzers: Rechte, Privilegien, Erwartungen
- Rechte und Privilegien der Institution
- Sicherheitsvoraussetzungen
- Arbeitnehmer-Regelung bzgl. Zuständigkeiten, Rechten, Nutzung und Datenschutzproblematiken
- Auswahl eines Mobile-Device-Management (MDM) Programms
- Vorsehen einer Möglichkeit zur Ortung (GPS) und Löschung verloren gegangener oder gestohlener Geräte

Ähnlich Schritte empfehlen auch Zahadat et al. in ihrer Planungsphase [vgl. 51, S.85 f.]:

- Identifikation der potentiellen BYOD-Nutzer und welche Ressourcen sie vermutlich abfordern.
- Formulierung von Standards zur Bestimmung welche Geräte die notwendigen Voraussetzung zur Teilnahme am Programm erfüllen und Festlegung zur Aufrechterhaltung der Aktualität dieser Standards.
- Auswahl einer Management-Software mit Remoteverwaltung von Applikationen und Einstellungen.
- Im sogenannten Asset-Management wird festgelegt, was die Institution gerne schützen möchte. Dazu werden alle Prozesse rund um den BYOD-Lifecycle betrachtet und schützenswerte Assets identifiziert.
- Untersuchung der Netzwerkumgebung (spezielle Funktionen wie Firewalls, Access-Control Lists (ACL)[1], Virtuelle LANs (VLANs)[2], Zoning[3], VPNs (siehe Kap.2.3.3) und Application Wrapping[4]) und Festlegung der Zugriffspunkte für die BYOD-Umgebung.

[1] Differenzierte Zugriffssteuerung auf Dateiebene
[2] Auftrennung physischer Netze in Teilnetze
[3] Unterteilung von Speichernetzen in einzelne, autarke Teilnetze
[4] Schutz von Anwendungen durch verschlüsseltes Verpacken in einer anderen Anwendung.

- Identifizierung der Richtlinien, Prozesse und Prozeduren für den Betrieb und die Überwachung des BYOD-Programms. Zur Festlegung der notwendigen Regularien sollte grundlegendes Wissen über die Grenzen der technischen Sicherheitsfunktionen im Zusammenhang mit BYOD dabei helfen, das richtige Maß an organisatorischen Mitteln zu bestimmen.

Zum besseren Verständnis des Bedarfs empfiehlt MobileIron an dieser Stelle eine kurze Befragung der Mitarbeiter mit folgender Zielsetzung [vgl. 34, S.5]:

- Vorlieben für Gerätetypen/Betriebssysteme ausmachen
- Motivationsfaktoren und Hemmnisse für BYOD-Teilnahme identifizieren
- Favorisierte (Unternehmens-)Apps feststellen
- Einflüsse von BYOD auf Produktivität und Privatleben erkunden

Sobald diese Untersuchungsergebnisse ausgewertet sind, ist nach MobileIron weiter zu prüfen, ob innerhalb der Institution auch die erforderlichen Mitarbeiter-Ressourcen zur Verfügung stehen. Dazu sollte eine Fähigkeitsanalyse durchgeführt werden. Die technischen Fähigkeiten, die für eine mobile IT-Infrastruktur von Nöten sind, unterscheiden sich nach der Einschätzung von MobileIron erheblich von der einer klassischen IT-Struktur einer Institution, weshalb dies Spezialwissen erfordert. Dieses Wissen kann bei den Mitarbeitern bereits vorhanden sein oder mittels Fortbildungen hergestellt werden. Es ist jedoch auch möglich, dass neue Mitarbeiter mit entsprechenden Qualifikationen benötigt werden. Mittels der Analyse soll festgestellt werden, ob für einzelne Aufgaben genügend Mitarbeiter vorhanden bzw. aktuell in Ausbildung sind oder noch fehlen [vgl. 34, S.6].

2.2.2 Einführung des Programms

In dieser Phase beginnt nach Zahadat et al. der BYOD-Lifecycle mit der Anmeldung (Register). Die Geräte, die am Programm teilnehmen sollen, werden vorgelegt, auf ihre Eignung hin geprüft und registriert. Vor Freischaltung, empfehlen Zahadat et al. zusätzlich eine Mitarbeiter-Schulung zu Regelungen, Abläufen und besonderen Rechten und Pflichten im Zusammenhang mit BYOD. Im Anschluss werden in der Bereitstellung (Provision) automatisiert die notwendigen Konfigurationen, Einstellungen, Applikationen und Zertifikate auf das Gerät übertragen, um alle Sicherheitsmechanismen des BYOD-Programms realisieren zu können [vgl. 51, S.86].

MobileIron empfiehlt die BYOD-Einführung in 3 Phasen vorzunehmen [vgl. 34, S.14]:

- **Pilotphase:** Testen mit einer kleinen Gruppe zur Einschätzung von Leistung, Support und sonstigen Problemen.
- **Bereitstellungsphase:** Schrittweise Vergrößerung des Teilnehmerkreis und Anpassung der Ressourcen..
- **Nachhaltigkeitsphase:** Optimierungen und Aufgabenübertragung vom Einführungsteam.

Nachdem die Benutzer und die Geräte zur Teilnahme am Programm vorbereitet wurden, geht es nun im Betrieb (Operate) um die Zielsetzung, die Geräte und die darauf befindlichen institutionellen Informationen zu schützen. Folgende Maßnahmen finden bei Zahadat et al. dazu Erwähnung [vgl. 51, S.86 ff.]:

- **Authentifikation** durch Zwei-Faktor-Eingabe verbessern
- **Funksicherheit** durch Verschlüsselungstechnik (WPA2 AES) erhöhen
- **Netzwerkarchitektur** umstrukturieren, dass BYO-Geräte besser identifizierbar sind
- **Sensibilisierung und Schulung** der Mitarbeiter speziell zu BYOD-Aspekten mit Eigenverantwortung
- **Application Store** ggf. mittels White-/Blacklists einschränken oder Verwendung eines expliziten Enterprise-Stores
- **IPSec/VPN** zur sicheren Kommunikation ggf. begrenzt auf einzelne Apps einsetzen
- **Management-Lösung** zur Geräteverwaltung mit besonderer Sorgfalt hinsichtlich der involvierten Administratoren (Qualifikation und Vertrauenswürdigkeit) einsetzen
- **Standortabhängige Funktionen** wie GPS-Funktionen nutzen um beispielsweise die Funktion von Kamera/Mikrofon an bestimmten, sensitiven Orten zu begrenzen und damit eine höhere Akzeptanz als durch Verbote erreichen
- **Fingerprinting** ggf. ergänzt durch MAC oder Seriennummer als zusätzlichen Vektor für die Authentifizierung einsetzen
- **Sandboxing** schützt davor, dass Daten aus einer geschützten Umgebung isoliert werden
- **Virtualisierung** ermöglicht ein hohes Maß an Kontrolle über die bearbeiteten Informationen, da die Daten die Institution nicht verlassen, sondern nur ein Videosignal an den BYOD-Client übertragen wird

- **Betriebssystem-Updates** beheben in der Regel Fehler, können aber auch neue Sicherheitslücken produzieren, weshalb die Institution entscheiden sollte, ob Updates nur via Management-Lösung oder auch durch den Benutzer selber installiert werden können

- **App-Updates** sollten regelmäßig durch den Benutzer selber installiert werden

Die von Zahadat et al. genannten Maßnahmen bieten Aspekte, die im Zusammenhang mit BYOD seltener erwähnt werden:
Eine Zwei-Faktor-Authentifikation stellt in Form einer PIN in Kombination mit einer zusätzlich benötigten Eingabe die momentan gebräuchliche Variante dar. Interessant ist die Betonung auf die Eignung des Personals zur Betreuung der Management-Lösung sowohl in fachlicher als auch menschlicher Hinsicht. Sicherlich ist es von Zahadat et al. nicht verkehrt, den großen Einfluss, den eine Management-Lösung auf verwaltete Geräte und die darauf gespeicherten Informationen hat, entsprechend zu thematisieren. Standortfunktionen wie GPS werden zumeist nur mit Ortungsdiensten etwa bei Verlust oder Diebstahl des Gerätes in Verbindung gebracht. Zahadat et al. liefern hier mit der Möglichkeit, aus Sicherheitsgründen, standortbezogen Funktionen deaktivieren zu können (Geofencing), weitere attraktive Einsatzoptionen. Die Nutzung von Fingerprinting als weiterer Faktor zur Authentifizierung ergänzt die nutzerzentrierten Eingabevariablen um eine gerätespezifische Komponente. Während zudem manches Mal dazu geraten wird, Updates möglichst umgehend zu installieren, erinnert Zahadat et al. daran, dass übereiltes Installieren im Einzelfall auch neue Sicherheits- oder Stabilitätsprobleme hervorrufen kann.

Zahadat et al. betonen, dass sich das BYOD-Programm immer wieder auf neue Bedrohungen anpassen muss: „Even when devices are adequately protected, changes in the technological landscape cause new attack vectors to arise daily.“ [51, S.89] Deshalb wird die Etablierung folgender Disziplinen empfohlen [vgl. 51, S.89 f.]:

- **Sicherheitslücken** der eingesetzten Geräte erkennen und feststellen welche Komponenten sie verursachen

- **Schadsoftware (Malware)** kann bei BYOD aufgrund der Nutzung öffentlicher Netze und den umfangreichen Benutzerrechten vermehrt auftreten und kann Unternehmens- oder Nutzerbasiert (auf dem Client) bekämpft werden

- **Angriffserkennung** soll dazu dienen, mittels Anomalieerkennung (Detection/Prevention System) oder intelligenter Firewalls im Netzwerk verdächtige Vorgänge zu erkennen, die auf nicht erkannte Sicherheitslücken oder Malware zurückzuführen sind

- **Geräteverlust** sollte, ganz gleich ob verloren oder gestohlen, zu einer sofortigen Meldung durch den Nutzer führen, was eine ausreichende Kenntnis über die Abläufe erfordert (Schulung)

- **Datenverlust** erkennen und vorbeugen durch ein sogenanntes Data Loss Prevention (DLP)-System[5], dass entweder in einer VPN-Kette den Datenstrom auf Auffälligkeiten hin prüft oder auf dem Client selber betrieben wird

- **Geräteüberwachung** wird vor allem dadurch eingeschränkt, als das der Benutzer der Eigentümer ist und zudem auch private Informationsströme über das Gerät laufen, die die Institution aufgrund rechtlicher Regelungen nicht überwachen darf

Diese eher theoretisch und oberflächlich gehaltene Auflistung von Maßnahmen zeigt recht deutlich die Schwierigkeit einer standardisierten Überwachung der BYO-Geräte und deren Kommunikation. Zu unterschiedlich sind die eingesetzten Systeme und deren Anwendungsszenarien. Zusätzlich liegt die Kommunikationskette in der Regel auch nicht vollständig im Einflussbereich der IT-Administration.
Das Problem thematisiert auch Tokuyoshi: „Remote devices connecting to arbitrary networks may place corporate data at risk. Without some protection in place to secure network traffic, the information is about as private as a postcard, open to anyone to read if they make the effort to look.“ [47, S.12] und nennt zwei Probleme: „First, the endpoint may need better security to protect against dangerous content; and second, network security measures can play a larger role in protecting the device as well.“ [47, S.12] Endgeräte-Absicherung ist nach Tokuyoshi bei BYOD manchmal ohne Alternative: „Endpoint security should be considered a measure of last resort, but with BYOD it's sometimes the only resort. If network security is not filtering out dangerous content, then the endpoint security is the only thing available to provide protection.“ [47, S.13] Weiter bezeichnet Tokuyoshi aber BYO-Geräte und deren Position außerhalb der Institution als „Wildcards“ [47, S.13], da man nie genau wissen kann, welche Sicherheitsmaßnahmen auf den Geräten und im Netzwerk implementiert sind. Er sieht deshalb einen Lösungsansatz darin, dass Institutionen das Handling von Datenströmen restriktiver handhaben sollten: „Organisations can tackle both sides of the issue – the network and the device – taking greater control and bringing clarity to what is known and unknown, and that's a much stronger position than trying to manage that which cannot be seen.“ [47, S.13] Er nennt dazu ein Beispiel, dass Netzwerkverkehr, der über einen gültigen Port läuft, aber im Grunde unbekannt ist, eher durchgelassen als blockiert wird. Unbekannt bedeutet dann also eher nicht gefährlich. Tokuyoshi meint dazu: „Starting with an assumption that unknown elements are not trusted can provide greater measures of precision

[5] Marketingbegriff für eine Software und/oder Hardware, die Datenströme untersucht und bewertet. Der Einsatz eines DLP im Unternehmen ist gegebenenfalls Datenschutzrechtlich problematisch.

about who can access particular resources, and that plays strongly into solving BYOD issues as well.“ [47, S.13]

Zahadat et al. nennen weiter eine Reihe von Aktionen, die im Falls eines Sicherheitsvorfalls zur Verfügung stehen sollten [vgl. 51, S.90]:

- **Beseitigung der Sicherheitslücke** mit Reaktion je nach Typ und Risiko des Problems
- **Entfernung von Schadprogrammen** je nach Gefährdung (potentiell oder akut schädlich) durch selektives Löschen bis hin zum „Wipe“.
- **Reaktion auf einen Vorfall** gemäß dem „Incident Response Plan (IRP)“ angepasst an die eingeschränkten Kontrollmöglichkeiten bei BYO-Geräten unter Erfordernis entsprechend geschulter Mitarbeiter
- **Deaktivierung eines Geräteaccounts** nach Meldung von Verlust oder Diebstahl
- **Entfernte Löschung (Wipe)** bei Verlust oder Diebstahl in vollständiger (rechtlich problematisch) oder selektiver (auf die institutionellen Informationen beschränkte) Form

Im Grunde beschränken sich die möglichen Aktionen, die Zahadat et al. als reaktive Möglichkeiten nach dem Eintritt eines Sicherheitsvorfalls nennen, auf eine Löschung der App oder einen teilweise bzw. vollständigen „Wipe“ des Geräts. Damit die institutionellen und ggf. auch privaten Informationen in der Folge nicht vollständig verloren sind, sollten im Vorfeld auch Wiederherstellungsmöglichkeiten geprüft werden. Dazu gehören nach Zahadat et al. [vgl. 51, S.90-91]:

- **Instituts-Backups** können, mit möglichen rechtlichen Problemen der Speicherung von privaten Mitarbeiterdaten auf Institutions-Servern, vollständig ausgeführt oder sich auf die institutionellen Informationen beschränkt werden
- **Mitarbeiter-Backups** können ebenfalls vollständig auf Speicher der Mitarbeiters oder Cloud-Speicher stattfinden und somit das Risiko mit sich bringen, das institutionelle Daten außerhalb der Institution abgelegt werden
- **Geräteverfolgung** kann dabei helfen festzustellen, ob ein Gerät nur verlegt oder verloren bzw. gestohlen wurde, stellt jedoch rechtlich auch eine gewisse Schwierigkeit dar, da diese Funktion als Mitarbeiterbeobachtung missbraucht werden könnte

Abschließend nennen Zahadat et al. noch die Aktivitäten, die ein BYOD-Programm zur Optimierung begleiten sollten [vgl. 51, S.91-92]:

- **Überprüfung und Evaluation des BYOD-Programms** hinsichtlich Effizienz und Aktualität in einem wiederkehrenden Zyklus von maximal einem Jahr
- **Gefährdung durch Insider** aus dem Institutionsumfeld erkennen, da diese durch ihr Wissen (je nach Position in der Institution) zudem einen Vorteil gegenüber externen Angriffen haben
- **Penetrations-Tests** zur Entdeckung von Sicherheitslücken sollten vorzugsweise auf institutionseigenen Geräten simuliert werden
- **Regelmäßige Überprüfung der Liste unterstützter Geräte** zur Anpassung an neue Sicherheitsstandards
- **Zulassung neuer Geräte**, die auch durch die Mitarbeiter eingereicht werden könnten, anhand festgelegter Kriterien
- **Gerät abmelden** durch vollständiges Zurücksetzen oder Löschung der relevanten Daten (Zugriffe, sensitive Daten, Zertifikate und Einstellungen sowie Sicherheitssoftware) wenn etwa ein Mitarbeiter die Institution verlässt

Kohne et al. empfehlen in diesem Zusammenhang die Etablierung eines „kontinuierlichen Verbesserungsprozesses“. [27, S.205] „Im Rahmen dieses Prozesses werden alle internen und externen Dienstleistungen, Prozesse, Projekte und Produkte permanent überwacht und mögliche Verbesserungen diskutiert. Diese Verbesserungsvorschläge können zum einen durch Lessons Learned[6] oder zum anderen durch internes oder externes Feedback eingehen.“ [27, S.205]

Zur Sicherung eines nachhaltig erfolgreichen Betriebs des BYOD-Programms, nennt MobileIron ergänzend noch zwei zusätzliche Faktoren, die gleichermaßen der Effizienzsteigerung wie auch der Kostenoptimierung dienen [vgl. 34, S.17 ff.]:

- **Selbsthilfe als Ergänzung zum Helpdesk-Support:** Ein zentraler Mechanismus zur Erhöhung der Benutzerzufriedenheit und zugleich zur Senkung von Supportkosten ist der Aufgabentransfer an den Mitarbeiter selber. Bestes Beispiel ist ein Registrierungsprozess, den der Mitarbeiter selber vornehmen kann. Dies entlastet die IT-Abteilung und gibt dem Mitarbeiter zugleich einen schnellen Zugang. Auch für Probleme einfacher Art sind Selbsthilfe-Portale eine gute Lösung. Einen qualifizierten Support ersetzen diese Lösungen jedoch nur teilweise, weshalb dieser ebenfalls vorhanden sein sollte.
- **Kostenoptimierung:** Das BYOD-Programm sollte von einer kontinuierlichen Kostenoptimierung begleitet werden. Dies umfasst die betrieblichen Abläufe wie dem Support durch Selbsthilfe als auch Möglichkeiten zur Kostenreduktion

[6] Treffen mit allen Beteiligten um Fehler, Gefährdungen und weitere Erkenntnisse zu sammeln und zukünftig zu vermeiden.

bei Datentarifen oder Gerätepreisen. Auch Haftungskosten und steuerliche Aspekte sollten bei der Strategie von (teil-)subventionierten Geräte in Betracht gezogen werden.

Zusammenfassend lässt sich aufgrund der Untersuchungsergebnisse festhalten, dass der Prozess zur Etablierung eines BYOD-Programms einer umfassenden Planung bedarf. Wenn das Projekt erst einmal ins Rollen gerät, sollte die Institution viele auftretende Fragestellungen bereits im Vorfeld durchgespielt haben. Gleichzeitig wird aber auch deutlich, dass es sich um einen dynamischen Prozess handelt, der regelmäßige Überprüfung und Nachjustierung benötigt. Der Einsatz einer Management-Lösung ist ab einem bestimmten Funktionsumfang aus rechtlicher und funktionaler Sicht unumgänglich. Gerade hinsichtlich des kritischen Ereignisses eines Geräteverlusts werden diese zusätzlichen Funktionen benötigt. Außerdem wird regelmäßig die Notwendigkeit zur Einbeziehung des Mitarbeiters thematisiert. Vor allem technische Grenzen führen immer wieder als Lösung darauf zurück, dass bestimmte Szenarien über Richtlinien auszuschließen sind.

2.3 Relevante Strategien/Techniken zur Umsetzung

Hinsichtlich der Umsetzung in die Praxis gilt es bei BYOD passende Strategien für die jeweiligen Infrastrukturen zu finden. Nicht jede Institution hat die Anforderung BYOD im vollen Funktionsumfang zu betreiben. Somit ist es auch durchaus denkbar nur Teilfunktionen zu integrieren. Als Grundlage haben aktuell zumeist die in den folgenden Unterkapiteln dargestellten Techniken und Vorgehensweisen Relevanz.

Hinsichtlich einer Sicherheitslösung für BYOD empfehlen Vignesh und Asha ein Modell mit unterschiedlichen Ebenen (Abb.2.5): „The multilevel security policy is made up of three levels – Organizational level, Application level and Device level policies.“[48, S.513]

- **Ebene 1 - Organization Level:** Diese Ebene sollte nach Vignesh und Asha genommen werden, bevor das BYOD-Programm startet. Anhand einer Checkliste sollte die Institution prüfen, ob sie ausreichend vorbereitet ist. Mögliche Punkte wären nach Vignesh und Asha beispielsweise: [vgl. 48, S.513]
  - Festlegen der Zuständigkeiten für Geräteunterstützung, -unterhalt und -kosten
  - Klarstellung das der Nutzer für das Sichern seiner privaten Daten zuständig ist
  - Mitarbeiter müssen bestimmte Apps auf Initiative der Institution entfernen

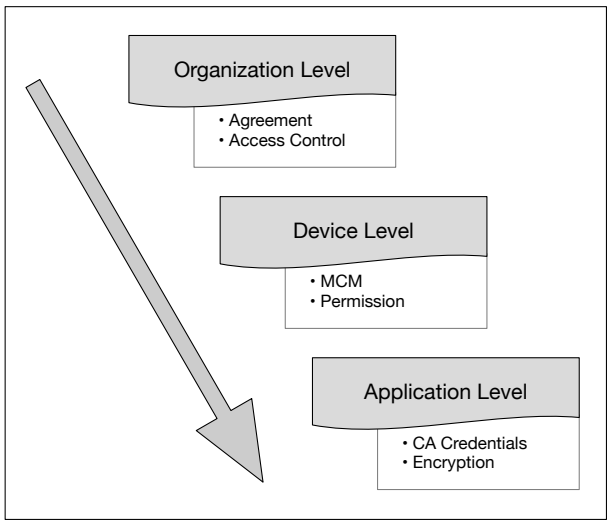

Abbildung 2.5: Multilevel Security Policy

  - Mitarbeiter darf kein modifiziertes (Rooted/Jailbreak) Gerät nutzen
  - Folgen von Verstößen gegen die Richtlinien erläutern
  - Zugriffsschutz auf institutionelle Daten je nach Position und Rang des Mitarbeiters
  - Nutzung des Fingerabdruck-Scanners zur Registrierung und zum Zugriff auf das Unternehmensnetzwerk
  - Mitarbeiter sind nicht dazu verpflichtet ihr eigenes Gerät mit zur Arbeit zu bringen

- **Ebene 2 - Application Level:** Auf dieser Ebene soll durch Nutzung von Software-Techniken das Sicherheitsniveau weiter erhöht werden. Als zentrales Werkzeug sehen Vignesh und Asha eine MDM-Software: „The Mobile Device Management supports full device control like lock down, control, SSL connection to the server, remote wipe, siren, signal flare and personal data backup and enforces policies even on mobile devices.“[48, S.514] Weiter wird eine Container-Lösung zur Absicherung sensitiver Informationen empfohlen: „The MDM should include MCM Mobile Content Management which is most important when handling sensitive information in the devices.“[48, S.514] Außerdem sollte zusätzlich eine Protokollierung und Restriktion zu installierender Apps erfolgen [vgl. 48, S.514].

- **Ebene 3 - Device Level:** Vignesh und Asha bemerken, dass viele Institutionen der Auffassung sind, dass Geräte-Richtlinien individuell vom Benutzer

> und Hersteller abhängen [vgl. 48, S.515]. Dieser Kategorie ordnen sie im weiteren Verlauf folgende Faktoren zu: „Some device level policies are Certificate authority, data encryption, multiuser and rooting issue.“[48, S.515]

Vignesh und Asha gehen davon aus, dass mit der Beachtung dieser drei Ebenen ein gutes Sicherheitsniveau realisiert werden kann, weisen aber zugleich auf die Notwendigkeit einer regelmäßigen Anpassung und Optimierung hin:

> „By adopting the three levels of security policy: Device level, Application level and Organization level; the level of security has increased and the organizations are in the safe zone while using BYOD. The devices are upgrading every period of time and different features are made available in the smartphones. The organization should change their trivial security policies and adopt the enhanced security policies to suit the mobile devices.“[48, S.515]

Im Folgenden werden einige der angesprochenen Aspekte dieser Ebenen detaillierter betrachtet.

2.3.1 Organisatorische Regelungen

Abseits technischer Mechanismen ist gerade bei BYOD das Sicherheits-Bewusstsein des Anwenders von zentraler Bedeutung für das Gelingen der Strategie. Dies lässt sich einerseits durch Sensibilisierung mittels *Schulungen*, aber auch mittels vertraglich fixierter Sorgfaltsverpflichtungen etwa in Form von *Benutzerrichtlinien* bzw. *BYOD-Policies* erreichen.
Ein weites Feld, dass es in diesem Zusammenhang zu beachten gilt, ist die rechtliche Situation: „Mangels spezifischer gesetzlicher BYOD-Regelungen obliegt es allein den Arbeitsvertragsparteien, den rechtlichen und tatsächlichen Rahmen des Einsatzes zu gestalten, der mit einer Fülle von Regelungsnotwendigkeiten und noch weitestgehend ungeklärten Detailfragen zu unterschiedlichsten Rechtsgebieten einhergeht.“[35, S.20] In diesem Bereich müssen folglich individuelle, schriftliche Vereinbarungen getroffen werden. Im Rahmen dieser Arbeit werden rechtliche Aspekte etwa in Kapitel 3.1.3 nur in Auszügen behandelt. Es wird deshalb zur rechtssicheren BYOD-Umsetzung auf jeden Fall eine umfassende juristische Beratung empfohlen.
Hinsichtlich der Einführung einer BYOD-Policy ist es wichtig, dass der Mitarbeiter diese nicht als Reglementierung auffasst: „Die BYOD-Policy sollte als gegenseitiges Entgegenkommen verstanden werden: Der Anwender sieht ein, dass der Arbeitgeber seine Daten schützen muss und der Arbeitgeber sieht ein, dass es sich um private Endgeräte handelt.“[27, S.16] Nach Kohne et al. gilt es, unabhängig vom Standort, vor allem zwei Grundsätze zu regeln [vgl. 27, S.16]:

- Anwender müssen der Institution eine eindeutige Erlaubnis zum Zugriff auf persönliche Daten geben.

- Institutionen müssen sensitive, persönliche Daten, die verarbeitet werden nach neustem Stand der Technik schützen.

Das Aufsetzen schriftlicher Vereinbarungen zum Thema BYOD ist ein individueller Vorgang. Kohne et al. empfehlen die Umsetzung der Regelungen in verschiedenen Dokumenten [vgl. 27, S.17 ff.]:

- **BYOD-Policy:** In diesem Dokument werden vier Bereiche abgedeckt. Die *Berechtigungsregeln* definieren, wer genau BYOD in welchem Umfang betreiben darf. Der Umgang mit privaten Daten auch im Notfall, die Installation von Management-Programmen und deren Einschränkungen von anderen Apps sowie die Notwendigkeit einer Datenverschlüsselung sind Bestandteil dieses Teils. Einen weiteren Abschnitt bilden die *Finanzierungsregeln*, die festlegen, wie das Gerät angeschafft wird (beispielsweise mit Subventionierung) und ob bzw. in welchem Umfang sich die Institution an den laufenden Kosten des Mobilfunkvertrags beteiligt oder diesen stellt. Letztlich gehören noch *Betriebsregeln* zu diesem Dokument, die Hinweise zur verpflichtenden Nutzung einer Management-Software, den Zuständigkeiten zur Anfertigung eines Backups, dem Ablauf für Ersatzgeräte bei Verlust oder Defekt sowie dem Umfang von Support-Leistungen geben.

- **BYOD-Vertrag:** Dieses Dokument referenziert die anderen Policy-Dokumente und muss von jedem Mitarbeiter, der BYOD betreiben möchte, akzeptiert und unterschrieben werden. Hier wird auch festgelegt in welcher Weise der Mitarbeiter das BYOD-Programm wieder verlassen kann und wie der Prozess dann genau aussieht.

- **Acceptable Use Policy:** Die Regelung, was der Mitarbeiter mit seinem Gerät in verschiedenen Einsatzszenarien darf und was nicht, ist Gegenstand dieses Dokuments. Dazu gehören beispielsweise private Nutzung während der Arbeitszeit, das Verbot des Einsatzes modifizierter Betriebssysteme, erlaubte private Apps (Sperrlisten) sowie mögliche andere Nutzer aus dem privaten Umfeld.

- **Security Policy:** Dieses Dokument widmet sich explizit dem Schutz der institutionellen Informationen auf dem Gerät. Dazu werden, teilweise auch gerätespezifisch, detaillierte zu Themen wie Verschlüsselung, Logging, Ortungsfunktionen, Löschung, Virenschutz, Komplexität der eingesetzten Authentifizierung sowie Deaktivierung von Gerätefunktionen wie etwa der Kamera an bestimmten Orten festgelegt.

- **Enterprise Mobility Management Strategie:** Nur zur internen Verwendung für die IT regelt dieses Dokument die technischen Details des Geräte-Managements.

Kohne et al. betonen zugleich, dass die Erstellung dieser Dokumente allein nicht ausreicht:

> „Sie müssen alle gemeinsam dafür Sorge tragen, dass die Vorgaben auch umgesetzt und die Regeln eingehalten werden (Policy to Process). Dies gilt für die IT, die die entsprechenden Vorgaben technisch umsetzen und überwachen muss, genauso wie für den Anwender, der die Geräte und Daten sorgfältig behandelt. Nur so kann ein erfolgreicher BYOD-Einsatz sichergestellt werden.“[27, S.23]

Diese umfangreiche Auflistung der Details, die nach Kohne et al. bei einer individuellen Anfertigung einer BYOD-Richtlinie Beachtung finden sollten, illustrieren die Vielschichtigkeit der Themen, die im Vorfeld zu bearbeiten sind. Gleichzeitig wird aber aus dem zuletzt geäußerten Statement auch wieder deutlich, dass trotz aller Regelungen der BYOD-Nutzer eine große Verantwortung für das Gelingen des BYOD-Programms trägt. Ergänzend zu diesem Thema liefert Monsch ein Muster für eine Nutzungsvereinbarung [vgl. 35, S.176 ff.], die eine gute Vorlage zur Erstellung eigener Dokumente darstellt.

2.3.2 Verschlüsselung für Datendienste

Beim einfachen Versand von E-Mails werden die Informationen im Klartext über das Internet versendet. Diese Variante ist folglich hinsichtlich Abhören und Modifikationen (Vertraulichkeit und Integrität) recht ungeschützt. Aus diesem Grunde wird die Verschlüsselung via *TLS* bei der Nutzung von E-Mails zunehmend empfohlen. Gleiches gilt auch für ähnliche Dienste wie Kontakte, Termine, Aufgaben und Notizen. Diese Datendienste lassen sich auch mit dem Begriff „Personal Information Manager (PIM)“ zusammenfassen.
TLS steht grundsätzlich für *Transport Layer Security*, ist ein hybrides Verschlüsselungsprotokoll zur Datenübertragung im Internet und basiert auf seinem Vorgänger *SSL* (*Secure Sockets Layer*). Es handelt sich nicht um eine explizite E-Mail-Verschlüsselung, sondern lediglich um eine Transportverschlüsselung zwischen den Servern: „SSL/TLS entstand zum Schutz des Datentransfers zwischen Browser und Webserver, sichert heute aber etwa auch den Datentransport zwischen Mail-Client und -Server.“[42, S.2]
Es existieren zwar Angriffe auf SSL/TLS, die Spezifikation und Implementierung wurde aber immer weiter verbessert, so dass aktuelle Versionen als sicher eingeordnet werden können: „SSL und TLS bieten, richtig eingesetzt, eine hohe Sicherheit.“[43,

S.178] Das Angriffsszenarien trotzdem Bestand haben zeigen beispielsweise Assing und Cale anhand verschiedener Szenarien wie etwa *man in the middle* [vgl. 4, S.35 ff.]. Bei der Nutzung von TLS zur E-Mail-Kommunikation erfolgt standardmäßig nur die Übertragung verschlüsselt. Einige Parameter müssen die E-Mail-Server im Vorfeld noch unverschlüsselt aushandeln. Um diese potentielle Sicherheitslücke zu umgehen, gibt es mit *STARTTLS* und *implizitem TLS* zwei Varianten, die eine frühere Verschlüsselung einleiten. Die sicherste Variante ist das *implizite TLS*, welches jedoch ein Problem im Zusammenhang mit Firewalls, die auf der Anwendungsschicht analysieren, bekommen kann. Dort liegt auch ein Problem: „Mit dem zunehmenden Einsatz von TLS 1.3 im Internet und in Firmennetzen wird es immer schwieriger, den Inhalt der Kommunikation im Netzwerk zu überwachen, um Fehlkonfigurationen und Angriffe zu entdecken."[33, S.96] Dadurch verschwinden, wie Mahnke und Frankenstein es nennen, auch die letzten Datenfetzen zur Erkennung von Malware und gezieltem Missbrauch und sehen einen Ansatz in der Betrachtung des gesamten Netzwerkverkehrs um Anomalien und typische Angriffsmuster auch weiterhin zu erkennen [vgl. 33, S.96].
Hinsichtlich der Nutzung im Zusammenhang mit BYOD dominieren die Vorteile einer SSL/TLS-verschlüsselten Kommunikation aber eindeutig. Die Verschlüsselung der E-Mail-Kommunikation ist für Geschäftskunden mittlerweile ohnehin verpflichtend. Dies regelt aktuell die DSGVO in Artikel 32 „Sicherheit der Verarbeitung"[7].
Für weitere Detailinformationen zu SSL/TLS sei auf Schwenk[43, S.147 ff.] verwiesen.

2.3.3 Virtual Private Network (VPN)

Auch wenn die Umstellung hin zum sogenannten IPv6-Standard für Netzwerke voranschreitet (in Deutschland aktuell knapp 60%[8], so basieren immer noch große Teile des heutigen Datentransfers auf IPv4. Zum Zeitpunkt der Entwicklung dieser Technik hat man sich noch wenig Gedanken über mögliche Angriffsszenarien gemacht. Kommt nur diese Technik allein zum Einsatz, ist es für versierte Angreifer recht einfach, Daten abzufangen und zu verändern.
Dem Bedarf nach einer sicheren Erweiterung des Unternehmensnetzes über öffentliche Kommunikationskanäle folgend, wurde mit dem sogenannten *Virtual Private Network (VPN)* eine Lösung entwickelt. *VPN* verschlüsselt den Datenstrom und gewährleistet Integrität und Vertraulichkeit. Die Verbindung wird über einen sogenannten *Tunnel* zwischen zwei Endpunkten über ein öffentliches Netz hergestellt. Mit Entwicklung leistungsstärkerer mobiler Geräte sind auch diese in der Lage den Mehraufwand der

[7] https://dsgvo-gesetz.de/art-32-dsgvo/
[8] `https://www.akamai.com/de/de/resources/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp`

VPN-basierten Kommunikation zu verarbeiten [vgl. 42, S.1]. Für den mobilen Client fühlt es sich mit *VPN* an, als ob er Teil des lokalen Netzwerkes wäre.
Um unterschiedlichen Anforderungen gerecht zu werden, gibt es verschiedene Verbindungsmodi im Zusammenhang mit *VPN*. Erwähnenswert hinsichtlich BYOD ist *Mobile VPN*. Die grundlegende VPN-Technik geht davon aus, dass sich während der Kommunikation über einen Tunnel die Netzwerke der beiden teilnehmenden Parteien nicht ändern. Bei einem mobilen Client, der beispielsweise in einem Zug eingeloggt ist, können sich die Zugangspunkte jedoch öfters ändern. Dazu wurde bei der *Mobile VPN*-Technik eine Instanz (Server) eingefügt, die die Verbindung zum Client vermittelt, auch über mehrere Zugangspunkte hinweg [vgl. 42, S.2].
Das *VPN*-Prinzip wird auch mit IPv6 fortbestehen. Bei IPv6 sind jedoch im Protokollstack bereits die für IPSec nötigen Extension Header integriert [9]. *VPN* gilt heute als sicherer *„de facto“*-Standard für die mobile Kommunikation mit dem Unternehmensnetzwerk. Für weitere Detailinformationen zu VPN sei auf Schwenk[43, S.89 ff.] verwiesen.

2.3.4 Remotezugang

Zum entfernten Zugriff auf den digitalen Arbeitsplatz wird bereits länger, etwa für Homeoffice-Tätigkeiten, auf eine Remotedesktop-Verbindung gesetzt. Bei dieser Variante der Virtualisierung stellt der mobile Client eine (in der Regel VPN-basierte) Netzwerkverbindung zu einem so genannten *Terminal Server* her. Dieser beherbergt eine vollständige Arbeitsumgebung samt Daten und Programmen. Zum mobilen Client wird lediglich ein Videosignal übertragen und der Austausch von Steuerbefehlen vorgenommen. Der mobile Client wird in diesem Fall als *Thin Client* bezeichnet. Ein Vorteil dieser Lösung ist, dass keine Daten das Unternehmensnetzwerk verlassen [vgl. 35, S.137] und die Administration deutlich erleichtert wird. Das dies auch für mobile Endgeräte Vorteile hat, betont Kretschmer: „Besonders viele Risiken und eher doppelt so hohe Kosten birgt der zunehmende Einsatz mobiler Endgeräte, die Folgekosten des Verlusts mobiler Geräte und darauf gespeicherter sensibler Daten nicht gerechnet.“[28] Bei der Verwendung so genannter *Fat-Clients* sieht sich die Administration dem „Sichern eines bunt gemischten 'Zoos' von Clients gegen alle Risiken“ [28] gegenüber gestellt. Nachteilig im Betrieb außerhalb der Institution ist die Notwendigkeit einer dauerhaften, ausreichend dimensionierten Datenverbindung und gegebenenfalls nicht angepasste Darstellung bzw. Eingabeoptionen für mobile Geräte: „Diese Technologie wurde für den Einsatz an klassischen PCs entwickelt und nicht für Endgeräte mit sehr kleinen Bildschirmen wie Smartphones oder Tablets.“[27, S.112] Kohne et al. raten deshalb dazu, im Zusammenhang mit BYOD die Verwendbarkeit im Vorfeld zu prüfen: „Hierbei ist es wichtig den Einsatz auf mehreren

[9] `https://www.ipv6-portal.de/informationen/technik/ipsec.html`

Geräten mit unterschiedlichem Formfaktor zu prüfen, um einen guten Überblick zu bekommen.“[27, S.113]

2.3.5 Container

Zur Absicherung von Firmendaten, sollten diese auf kombiniert beruflich und privat genutzten Geräten abgeschirmt werden. Dies hat sicherheitstechnische aber auch datenschutzrechtliche Gründe. Am besten lässt sich diese klare Trennung mittels einer *Container-Lösung* erreichen: „Der Begriff 'Container' bezeichnet eine Technik, bei der ein Wirtssystem mehrere Anwendungen parallel in separierten Umgebungen ausführt (Operating System Level Virtualization).“[12, S.1]
Container-Lösungen kommen im Zusammenhang mit BYOD zumeist als Bestandteil einer Management-Lösung (MAM bzw. EMM) zum Einsatz. Es gibt jedoch auch kleinere Lösungen, die keine Management-Lösung voraussetzen wie beispielsweise SecurePIM[10].
Technisch gesehen sind Container keine Neuheiten: „Im Prinzip sind Container nur chroot-Umgebungen, die man bei Linux seit den 1990ern kennt, oder Jails, die BSD Anfang des Jahrtausends einführte.“[39, S.108] Puppe vergleicht diese Lösungen mit der Sandbox von Java, warnt aber zugleich, dass solche Lösungen kein Allheilmittel darstellen: „Spätestens seit Rowhammer, Meltdown und Spectre in all seinen Varianten sollte jedem klar sein, dass geteilte Hardware immer ein Sicherheitsrisiko ist. Auch Ausbrüche aus Virtualisierung und Sandboxen gibt es ausreichend.“[39, S.108]

> „Die MDM-Lösungen der laut Gartner führenden MDM-Anbieter beinhalten zwar alle eine Umsetzung des Container-Konzepts, dennoch bieten diese Lösungen in der Regel auch nach wie vor noch die Möglichkeit, Konfigurationen insbesondere von sicherheitsrelevanten Einstellungen über den Container hinaus auch auf der Ebene des Gerätes vorzunehmen. Dies liegt darin begründet, dass die Sicherheit eines Containers immer auch von der Sicherheit des zugrunde liegenden Betriebssystems abhängt.“[27, S.83]

Deshalb urteilen Kohne et al. auch: „Das Container-Konzept an sich ist deshalb nicht als Sicherheitsfunktion zu betrachten, dank dessen sich Unternehmen bei der Verwaltung von Endgeräten nur noch auf den Container konzentrieren können.“[27, S.84] Vorteilhaft wird aber der Zugriffsschutz mit einer eigenen PIN/Passwort, die Möglichkeit der expliziten Verschlüsselung des Containers, die Option des einfachen Löschens von institutionellen Informationen (da gekapselt im Container) und der

[10] `https://www.virtual-solution.com/securepim/`

Trennung des Kontroll-Zugriffs zwischen institutionellen und privaten Informationen gesehen [vgl. 27, S.84].
Das BSI hat einen entsprechenden Baustein zu Containern in der Entwicklung. Aktuell liegt dieser als Community-Draft[11] vor und gibt einen Ausblick, was der zukünftige Baustein enthalten wird. Hierzu sei auch auf den Report von Puppe[39] verwiesen.

2.3.6 Mobile-Device-Management

Dem Wunsch der Kunden zur zentralen Administration von Devices, die primär im Consumer-Markt Einsatz finden, folgend, haben die Hersteller Schnittstellen (API) für so genannte *Mobile-Device-Management*-Systeme geschaffen. Damit ist es möglich, Geräte aus der Ferne (auch partiell) zu administrieren und beispielsweise bei Verlust oder Ausscheiden des Mitarbeiters via Remote-Befehl die betrieblichen (Corporate-Wipe) oder gleich alle Daten (Wipe) zu löschen. Die Vorkehrungen der Hersteller wie etwa von Google für Android[12] bzw. Apple für iOS[13] werden durch spezielle Software-Entwicklungen aufgegriffen und in Funktionalitäten umgesetzt.
Der Einsatz einer MDM-Lösung ist sehr zu empfehlen. „Nur (mit einer MDM-Lösung) kann gewährleistet werden, dass ein Unternehmen den Überblick über alle betrieblich eingebundenen Smartphones und Tablets behält und die zugehörigen Verwaltungsaufgaben unterstützt werden“ [27, S.79].

MDM-Angebote gibt es für die gängigen mobilen Betriebssysteme. Bei der Betrachtung der Lösungen gilt es vor allem zu vergleichen welche Betriebssysteme und Anforderungen unterstützt werden müssten, da sich die angebotenen Funktionsumfänge unterscheiden.
Auch wenn der Begriff eines *MDM* oft Verwendung findet, so handelt es sich zumeist um Lösungen, die noch über den Funktionsumfang eines *MDM* hinausgehen.
Für weitergehende Informationen sei auf das Kapitel 4.4 verwiesen.

2.3.7 Datenverschlüsselung

Zusätzlich zur Verschlüsselung der Kommunikation lassen sich auch die lokal gespeicherten Daten durch kryptographische Verfahren verschlüsseln. Dies stellt eine

[11] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Container.pdf?__blob=publicationFile&v=4
[12] https://developers.google.com/android/management/introduction
[13] https://developer.apple.com/business/documentation/MDM-Protocol-Reference.pdf

sehr wirksame Maßnahme dar, dass diese Informationen auch bei Verlust der Daten vertraulich bleiben. Grundsätzlich existieren diverse Möglichkeiten Daten zu verschlüsseln. An dieser Stelle sollen die Umsetzungen hinsichtlich der gängigen Betriebssysteme Betrachtung finden.
Allen Implementierungen zu Grunde liegt zunächst einmal ein kryptographisches Verfahren. Hierbei handelt es sich um ein symmetrisches Verfahren, basierend auf folgenden Standards:

- Der *Data Encryption Standard (DES)* ist das bei weitem bekannteste Verfahren der letzten 30 Jahre. Heutzutage ist DES aufgrund der zu geringen Schlüssellänge nicht mehr sicher. Mit 3-facher Verschlüsselung bei 3DES wird diese Weiterentwicklung auch heute noch verbreitet eingesetzt [vgl. 37, S.55].
- Als DES-Nachfolger wurde der *Advanced Encryption Standard (AES)* entwickelt um die Nachteile von DES hinsichtlich Blocklänge und Performance zu beseitigen. Der Initiator, das US National Institute of Standards and Technology (NIST), war der Auffassung, dass zur Zielerreichung eine Neuentwicklung notwendig sei. Im Jahr 2000 wurde der *Rijndael*-Algorithmus als zukünftiger AES gekürt [vgl. 37, S.88].
  Bei AES handelt es sich um ein symmetrisches Verfahren mit einer Blockgröße von 128 Bit. Wahlweise können Schlüssellängen von 128, 192 oder 256 Bit verwendet werden. Der Algorithmus lässt sich effizient in Software und Hardware umsetzen. Es sind bisher keine effizienteren Angriffe auf AES als Brute-Force[14] bekannt. AES ist Teil vieler Standards wie *IPsec oder TLS* [vgl. 37, S.117].

Problematisch bei allen Formen von Verschlüsselungs-Algorithmen ist die Qualität des Passworts, dessen Generierung und sichere Verwahrung. Um diesbezüglich einen „sicheren Hafen“ in den Computersystemen zu schaffen, wurden so genannte *TPM-Chips* implementiert: „Eine Trusted Platform muss in der Lage sein, wichtige Geheimnisse, Zertifikate, Schlüssel sowie kritische (kryptographische) Operationen sicher in einer geschützten Hardware-Umgebung zu speichern beziehungsweise auszuführen.“ [17] Das *Trusted Platform Module (TPM)* ist ein Chip, der nach der Spezifikation der *Trusted Computing Group (TCG)* entwickelt wurde und im Rechner diese grundlegenden Sicherheitsfunktionen bereitstellt. Er ist vergleichbar mit einer fest auf dem Motherboard verlöteten Smartcard und bietet eine funktionale Einheit (Zufallszahlengenerator, Hash, HMAC, RSA-Schlüsselgenerator und RSA-Ver-/Entschlüsselung), einen nicht-flüchtige Speicher für unveränderbare Schlüssel (Endorsement Key, Storage Root Key und Owner Auth Secret) sowie einen flüchtigen Speicher für beispielsweise temporäre Keys [vgl. 17].
TPM ist jedoch nicht unumstritten. Durch die theoretische eindeutige Identifizierbarkeit eines Rechners mit aktiviertem TPM-Chip, wäre es beispielsweise auch möglich *Digital Rights Management (DRM)* zu betreiben und Software fest an eine Hardware

[14] Versuch durch zufälliges Ausprobieren eine richtige Eingabe zu erraten.

zu binden. Weiter problematisch wird die Weiterentwicklung des Standards hin zu TPM 2.0 gesehen. Alte, unsichere Algorithmen wie etwas SHA-1 wurden zwar durch SHA-2 erweitert, der Einsatz von SHA-1 wird aber weiterhin ermöglicht. Dies war einer der Gründe, warum Deutschland bei der Abstimmung zum Standard gegen diesen gestimmt hat [vgl. 26, S.9]. TPM kommt aktuell in Windows 10 für Bitlocker, virtuelle Smartcards, Provable PC Health (SecureBoot) und Passport (Speicherung von Passwörtern) zum Einsatz [vgl. 41].
AES und TPM sind die Techniken, die die Windows Festplattenverschlüsselung *BitLocker* nutzt. TPM wird genutzt um die Vertrauenskette beim Systemstart herzustellen. BitLocker schaltet sich zwar schon vor dem Systemstart ein, stellt aber mittels TPM die Integrität der UEFI-Firmware sicher. Eine Nutzung auf Rechnern ohne TPM ist auch möglich; dann werden die Daten für die Prüfung der Integrität von einem USB-Stick eingelesen. Damit bietet BitLocker idealerweise System-Integritätsprüfung und Festplattenverschlüsselung in einem [vgl. 36, S.2]. Die Entschlüsselung läuft wahlweise mit dem TPM alleine, der Eingabe einer PIN und/oder dem Auslesen von Schlüsselmaterial von einem externen USB-Stick [vgl. 36, S.5].
Die Verschlüsselung mit BitLocker erfolgt mit AES-128 und bietet damit schon eine gute Sicherheit. Eine Verschlüsselung mit dem optional möglichen AES-256 lässt sich zwar auch realisieren, bringt aber keinen entscheidenden Sicherheitsgewinn: Wenn ein Brute-Force-Angriff auf AES-128 schon extrem lange dauert, dauert es mit AES-256 nicht entscheidend länger: „For example, if it would take a quadrillion years to brute-force 128-bit AES, does it really matter that it might take even longer to brute-force 256-bit AES? For all realistic purposes, they're equally secure.“[24] Dies ist zwar rechnerisch logisch, aber trotzdem gibt es Gründe für AES-256: Die NSA beispielsweise gibt für Dateien mit dem Zusatz „SECRET“ AES-128 und mit dem Zusatz „TOP SECRET“ AES-256 verpflichtend vor. So kann es folglich auch Standards geben, die AES-256 notwendig machen [vgl. 24]. BitLocker arbeitet per Default im Modus *CBC* (diffused). Der als noch etwas sicher geltende *XTS*-Modus ist seit Windows 10 ebenfalls möglich.
Das Pendant zu BitLocker bei macOS heißt FileVault und ist ebenfalls eine Festplattenverschlüsselung, die standardmäßig mit XTS-AES-128 arbeitet [vgl. 2, S.4].
Für aktuelle und ältere Betriebssystemversionen existiert zudem eine Open-Source-Software namens *VeraCrypt*[15], die sich aus dem im Jahre 2014 eingestellten Projekt *TrueCrypt* abgespaltet hat.
Wie bereits erwähnt nutzen sowohl Windows als auch macOS die Festplattenverschlüsselung. Dieses Verfahren schützt die Informationen auf dem Datenträger, indem dieser komplett verschlüsselt wird. Mit dem Start des Betriebssystems liegen die verwendeten Schlüssel im Arbeitsspeicher vor. Ein entwendetes Gerät ist nur dann sicher, wenn das System ausgeschaltet oder sich im Ruhezustand (Hibernation) befindet. Im Standby-Modus wäre es theoretisch möglich die Schlüssel im Arbeitsspeicher abzu-

[15] `https://www.veracrypt.fr`

rufen und zur Entschlüsselung zu benutzen. Es muss lediglich die Bildschirmsperre umgangen werden. Wie sieht das nun für mobile Betriebssysteme aus? Das Problem dabei ist, dass mobile Geräte in der Regel immer in Betrieb sind. „Apple bietet für iOS eine File-based Encryption, während Google lange eine Full-Disk Encryption bevorzugte." [21, S.117] Das lässt vermuten, dass iOS schon von der Architektur her grundsätzlich noch etwas besser abgesichert ist als Android. Das bestätigt auch Günther und Zimmermann: „Mit den letzten Android-Versionen schließt Google zwar auf, dennoch entspricht der Schutz nicht dem von iOS."[21, S.117] Das Problem führt Günther und Zimmermann wie folgt weiter aus:

> Weder schaltet man sein Gerät aus, bevor man es verliert, noch fährt man aktiv sein Smartphone herunter. In der Praxis bedeutet das: Hat der Anwender sein Passwort (Boot-PIN, Pre-Boot-Authentication) beim Starten eingegeben, hält Android den gesamten kryptografischen Schlüssel im Arbeitsspeicher, solange das Gerät Strom erhält und der Nutzer es nicht aktiv ausschaltet. So schützt die Verschlüsselung die Daten des Anwenders nicht besser gegen einen Angreifer, der während dieser Zeit - die der Normalzustand ist - das Smartphone in die Hände bekommt.
> Im Endeffekt stellt dies lediglich eine Bildschirmsperre dar. Eine solche lässt sich aber immer wieder mit einfachen Mitteln umgehen. Folglich ist die Verschlüsselung des Datenträgers der falsche Weg im mobilen Umfeld. Google hat dies erkannt und sieht das Verfahren seit einiger Zeit nicht mehr als primäres Instrument zum Schutz der im Speicher befindlichen Daten an. Stattdessen wendet sich Android bereits seit Version 7.0 der Dateiverschlüsselung zu [21, S.117].

Apple nutzt für die Verschlüsselung, die seit iOS 4 angeboten wird, immer schon die Dateiverschlüsselung mit einer hardwarebasierten 256-Bit-AES-Engine. Bei einer Dateiverschlüsselung kommt für jede Datei ein eigener Schlüssel zum Einsatz. Diese aufwändigere Variante ermöglicht eine detailliertere Zugangskontrolle. Die Sicherheit wird dabei mit Hilfe eines Co-Prozessors, der *Secure Enclave*, realisiert. Dieser erledigt unter anderem einen ähnlichen Job wie eine TPM. Bei Android gibt es eine solche hardwarebasierte Sicherheitsinstanz nicht. Eine Ausnahme stellen die Geräte des Herstellers BlackBerry dar. Dieser hat, ähnlich der Apple Secure Enclave, Schlüssel und Zertifikate fest auf die CPU gebrannt. Dieser erweiterte Schutz gleicht jedoch dem Funktionsumfang der Apple Secure Enclave nur im Ansatz. Auch andere Hersteller haben mittlerweile Sicherheitskonzepte für Android entwickelt: Beispielsweise Samsung Knox[16] oder LG Gate[17]. Auch Google hat mittlerweile mit Android Enterprise[18] sicherheitstechnisch für Unternehmen relevante Funktionen in

[16] `https://www.samsungknox.com/de`
[17] `https://www.lg.com/us/business/enterprise-mobility`
[18] `https://www.android.com/enterprise/`

Android integriert. Für weitere Details zu den aktuellen Sicherheitsfunktionen von Android und iOS sei an dieser Stelle auf die Hersteller-Informationen von Google[19] und Apple[20] verwiesen.
Abschließend lässt sich festhalten, dass sich aufgrund ihrer Nutzungsprofile bei Mobilgeräten die Dateiverschlüsselung als sinnvoll erwiesen hat, während bei klassischen Betriebssystemen die etwas einfachere Festplattenverschlüsselung ausreichend ist. Gemein haben beide Verfahren die Nutzung von AES-128 bzw. AES-256, die nach aktuellem Stand beide eine große Sicherheit bieten. Apple hat mit iOS historisch gesehen sicherheitstechnisch die bessere Verschlüsselung, während Android aber mittlerweile auch nachgezogen hat und seit Android 7 ebenfalls die Dateiverschlüsselung einsetzt.

2.4 Best-Practices

Am Beispiel verschiedener Institute, die teilweise bereits ein BYOD-Programm betreiben, soll die aktuelle Praxis untersucht werden.
Dazu wurde nach einer initialen Kontaktaufnahme in einem ersten Schritt ein Fragebogen als Gesprächsgrundlage entwickelt und übersendet. Dieser sollte vor allem dazu dienen, die Tiefe der gewünschten Informationen zu verdeutlichen.

Die Inhalte aus dem Fragebogen:

- **Strategie**
  - Liegt der Schwerpunkt aktuell eher im klassischen Home Office oder im Mobile Office?
  - Welche Dienste werden mit BYOD abgedeckt (z.B. Mail, Termine, Kontakte, Intranet etc.)?
  - Welche Daten sind für den Mitarbeiter im Rahmen von BYOD verfüg- bzw. nutzbar (z.B. Kundendaten)?
  - Gibt es spezielle (auf Mobilgeräte optimierte) Anwendungen/Apps?
  - Welche Probleme/Gefahren sind durch den Einsatz von BYOD entstanden?
- **Zugang**
  - Welche Mitarbeiter können BYOD betreiben?
  - Welche Voraussetzungen müssen erfüllt sein?

[19] `https://source.android.com/security`
[20] `https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf`

- **Technik**
  - Gibt es eine Beschränkung auf bestimmte Geräte? Falls ja, welche (Gerätetypen, Betriebssysteme)?
  - Wie wird der Zugang realisiert (z.B. VPN/Token)?
  - Wird ein spezielles Management-System zur Fernadministration (MDM) eingesetzt? Falls ja, welches?
  - Muss spezielle Software installiert sein (z.B. Antivirus)?
- **Regelungen**
  - Gibt es eine schriftliche Nutzungsvereinbarung (hinsichtlich Haftung)?
  - Müssen bestimmte Fertigkeiten (seitens des Mitarbeiters) erfüllt werden (z.B. Schulungen)?
  - Wie wird der Datenschutz der personenbezogenen Daten (auf Seiten des Mitarbeiters und evtl. verarbeiteter Kundendaten) sichergestellt?
  - Wie wird die Arbeitszeit des Mitarbeiters geregelt (Verfügbarkeit, „24/7“)?

Auf Basis der Gespräche wurde jeweils ein Protokoll angefertigt und zur Freigabe vorgelegt. Die Ergebnisse finden sich im Folgenden.

BYOD bei einem Institut aus dem Bankensektor 1

Im Gespräch mit dem Informationssicherheitsbeauftragten konnten folgende Ergebnisse gewonnen werden:

- **Strategie:** Das Institut bietet seinen Mitarbeitern mobile Zugänge in unterschiedlichen Ausprägungen als Zusatzleistung zum eigentlichen Arbeitsplatz an. BYOD-Dienste für tägliche Aufgaben wie E-Mail, Termine oder Kontakte können auf dem privaten Endgerät bereitgestellt werden. Weiter existieren auch einige eigene Apps, die auf die Mobilgeräte-Nutzung hin optimiert sind und im Rahmen von BYOD und firmeneigenen Geräten als „gemanagte“ Apps zielabhängig angeboten werden. Zugriff auf betriebliche Dateien wird nur für firmeneigene Mobilgeräte angeboten, da die rechtlichen Schwierigkeiten/Bedenken hinsichtlich einer ausreichenden Trennung und vor allem einer möglichen Remote-Löschung vom privaten Gerät momentan überwiegen. Die klassische VPN-Remoteverbindung (Citrix) auf den Account via Token-Authentifizierung stellt eine weitere Nutzungsvariante dar, die losgelöst von den BYOD-Regularien zur Verfügung steht. Durch die Einführung von BYOD neu entstandene Gefahren wurden nicht festgestellt.

- **Zugang:** Die Dienste, die im Rahmen von BYOD angeboten werden, können grundsätzlich von jedem Mitarbeiter genutzt werden. Voraussetzung ist, dass der jeweilige Leiter die Nutzung für diesen Arbeitsbereich für sinnvoll hält und seine Genehmigung erteilt. Die Nutzung der mobilen Geräte aus dem Bestand des Instituts zu privaten Zwecken wird den Mitarbeitern gestattet.

- **Technik:** Voraussetzung für die Zulassung zu BYOD-Diensten sind Geräte mit dem iOS-Betriebssystem (iPhone/iPad). Android-basierte Geräte sind aufgrund von Sicherheitsbedenken (Sicherheitsupdates, ungeregelte AppStores, MDM-Problematiken) momentan ausgeschlossen. Als Managementsystem (MDM) kommt die Software MobileIron zum Einsatz, die mittels Zertifikat verteilt wird. Durch diese technische Lösung wird auch sichergestellt, dass die verwendeten Geräte über aktuelle Versionen der Betriebssysteme verfügen. Weitere Sicherheitsmaßnahmen wie Virenscanner oder Firewalls werden aufgrund der Struktur von iOS nicht vorausgesetzt. Auf Seiten des VPN-Fernzugriffs gibt es aufgrund der unbeschränkten Gerätetypen organisatorische Anweisungen, die z.B. regelmäßige Updates und den Einsatz eines Virenscanners voraussetzen.

- **Regelungen:** Es existieren Nutzungsbedingungen für die verschiedenen Einsatzszenarien (BYOD, betrieblichen Geräten, VPN-Fernzugriff), die der Mitarbeiter vor Erteilung eines Zugangs akzeptieren muss. Hierin werden sowohl sicherheitstechnische, rechtliche als auch organisatorische Hinweise gegeben. Viele Regelungen (beispielsweise zum Datenschutz) sind jedoch ohnehin bereits im Vorfeld aufgrund der Tätigkeit im Bankensektor notwendig. Den Mitarbeitern, die BYOD betreiben möchten, wird ein Handbuch zur Benutzung zur Verfügung gestellt. Bei der Nutzung betriebseigener Geräte ist bei Ausgabe eine Mitarbeiterschulung obligatorisch. Seine Arbeitszeiten kann der Mitarbeiter selbstbestimmt verwalten; eine Abschaltung der Dienste am Wochenende oder im Urlaub findet nicht statt.

BYOD bei einem Institut aus dem Bankensektor 2

Durch Rückmeldung des Informationssicherheitsbeauftragten konnten folgende Ergebnisse gewonnen werden:

- **Strategie:** Das Institut bietet seinen Mitarbeitern im Rahmen von BYOD primär die Möglichkeit so genannte PIM-Dienste (Personal Information Manager, Software zur Verarbeitung von E-Mails, Terminen, Kontakten und Aufgaben bzw. Notizen) zu nutzen. Hierbei werden gegebenenfalls auch Kundeninformationen ausgetauscht. Die Nutzung des Intranets ist ebenfalls möglich, spielt aber eine eher zu vernachlässigende Rolle. Zur Sicherstellung einer positiven

Benutzererfahrung werden die bereitgestellten Dienste größtenteils über die nativen Apps des Betriebssystems abgebildet; nur wenige, spezielle Apps werden zusätzlich angeboten.
Durch die Einführung von BYOD neu entstandene mögliche Gefahren werden, soweit sie hinsichtlich der Häufigkeit des Auftretens und dem Maße der Auswirkungen akzeptabel sind, beobachtet und als latente[21] Risiken bewertet.

- **Zugang:** Mit Genehmigung des Vorgesetzten kann grundsätzlich jeder Mitarbeiter die Dienste, die im Rahmen von BYOD angeboten werden, nutzen. Zur Teilnahme reicht einzig die positive Einschätzung des Vorgesetzten. Weiteren Fertigkeiten müssen nicht nachgewiesen werden.
- **Technik:** Zugelassen zur Teilnahme am BYOD-Programm sind Geräte mit dem iOS-Betriebssystem (iPhone/iPad). Android-basierte Geräte werden nicht unterstützt. Die MDM-Software MobileIron kommt als Management-Lösung zum Einsatz und wird mittels Zertifikat verteilt. Auf diesem Wege wird auch festgestellt, ob die verwendeten Geräte über eine aktuelle Betriebssystem-Version verfügen. Die Verbindungen werden grundsätzlich auf VPN-Basis betrieben. Weitere Sicherheitsmaßnahmen wie die Nutzung eines Virenscanners oder einer Firewall werden nicht vorausgesetzt.
- **Regelungen:** Jeder Nutzer wird durch eine Verpflichtungserklärung auf seine Pflichten im Rahmen der Teilnahme am BYOD-Programm hingewiesen. Die Arbeitszeiten sind über eine Dienstvereinbarung geregelt; es gelten die üblichen Dienstzeiten. Der Datenschutz der personenbezogenen Daten wird über die technische Lösung des MDM in Form von Policies sichergestellt.

BYOD bei einer Hochschule

Auf eine Anfrage beim IT-Helpdesk der Hochschule signalisierte der Mitarbeiter generelle Bereitschaft zur Unterstützung. Zugleich wies er aber darauf hin, dass die Hochschule mit ihren vielen Unterbereichen hinsichtlich BYOD etwas heterogen aufgestellt sei.

- Im Rahmenkonzept zur Informationssicherheit der Hochschule wird das Thema BYOD nur rudimentär behandelt.
- Auch wenn die übersendeten Fragen als sehr spannend kommentiert wurden, konnten sie nicht beantwortet werden. Grund ist, dass die RUB sich derzeit nach eigener Aussage in einer internen Abstimmungs- bzw. Entscheidungsphase zum Thema BYOD befindet. Auch wenn dieses Ergebnis natürlich nicht

[21] Bezeichnung für etwas, was zwar vorhanden, aber (noch) nicht offensichtlich bzw. noch verborgen ist.

wünschenswert war, so zeigt es doch auch einen Ausschnitt aus der Praxis. Viele Institute wissen darum, dass dieses Thema mehr Regelung verlangt und arbeiten an Lösungen. Dies unterstreicht die Nützlichkeit eines Bausteins zu diesem Themengebiet.

BYOD bei einem IT-Dienstleister

Ein IT-Dienstleister, der Buchhaltungs-, IT- und Personal-Services für Wohlfahrt, Kirche und Gesundheitswesen anbietet, gab im Gespräch Auskunft zum aktuellen BYOD-Programm.

- **Strategie:** Das Unternehmen bietet seinen Mitarbeitern im Rahmen des BYOD-Programms Zugang zu Diensten aus Office365 und PIM (Personal Information Manager) mit Ausrichtung auf das „Mobile Office“. Geschäftsanwendungen sind nicht Bestandteil des Programms und laufen nur über die so genannte „Private Cloud“, die von Extern lediglich über Notebooks mit klassischer VPN-Remoteverbindung (Citrix) genutzt werden kann. Der Zugang für diese Geräte erfolgt mittels *Microsoft Authenticator* (One-Time-Pad). Spezielle Apps existieren beispielsweise zu Koordinations-/Abrechnungszwecken bei ambulanten Pflegediensten (Android-basiert), die allerdings nur für dienstliche Geräte zur Verfügung stehen und nicht für das BYOD-Programm angeboten werden.
  Als BYOD-spezifische Herausforderung beim Betrieb des Programms wurde das neu entstandene Spannungsfeld gemischter Verantwortung zwischen Institution und Mitarbeiter genannt: Auch mit technischer Unterstützung hat der Mitarbeiter mit dafür Sorge zu tragen, institutionelle und private Informationen auf seinem Gerät zu trennen. Die eingeschränkte Verwendbarkeit klassischer Policy-basierter Richtlinien zur Geräteverwaltung wurde als weiteres spezifisches Merkmal erwähnt, dass die Notwendigkeit zu neuen Lösungen unterstreicht.

- **Zugang:** Grundsätzlich haben alle Mitarbeiter die Möglichkeit am BYOD-Programm teilzunehmen; die Entscheidung über die Zweckmäßigkeit obliegt dem jeweiligen Vorgesetzten. Voraussetzung ist das Vorhandensein eines geeigneten mobilen Endgeräts.

- **Technik:** Die Mitarbeiter können aus einem regelmäßig aktualisiertem „Warenkorb“ ein Android- oder iOS-basiertes mobiles Endgerät auswählen. Dieses wird von der Institution bezuschusst um die Attraktivität des Programms weiter zu steigern. Außer der jeweils aktuellsten Version des Betriebssystems muss keine weitere Sicherheitssoftware (z.B. Antivirus) vorhanden sein.

Aktuell wird zum Management der mobilen Geräte auf die (auf *Microsoft Intune* basierende) MDM-Funktion von *Office365*[22] gesetzt. Dieses bietet MDM-typische Funktionen wie das verpflichtende Setzen von PINs und Passwörtern oder „Corporate-Wipe“ zum selektiven Löschen von Informationen aus der Ferne. Zukünftig soll mit der *baramundi Management Suite*[23] eine UEM-Lösung weitere Möglichkeiten erschließen.

- **Regelungen:** Eine Nutzungsvereinbarung existiert in Form einer Verfahrensanweisung, die jedoch keiner expliziten Zustimmung des Mitarbeiters bedarf. Der Umgang und das Verhalten im Zusammenhang mit BYOD wird den Mitarbeitern als ein Bestandteil im Rahmen der Informations- und Telekommunikationsrichtlinie vermittelt.
  Durch die Teilnahme am Programm verpflichtet sich der Mitarbeiter nicht zu einer erweiterten Erreichbarkeit. Eine Ausnahme gibt es nur bei Mitarbeitern des Service-Desks, die für eine initiale Kontaktaufnahme wahlweise auch BYO-Geräte nutzen können. Diese Erreichbarkeit wird jedoch im Rahmen der normalen Arbeitszeitenregelung abgedeckt.

[22] `https://news.microsoft.com/de-de/ab-sofort-mobile-device-management-mdm-in-office-365-mglich/`
[23] `https://www.baramundi.de/management-suite/ueberblick/`

3 Gefährdungen und deren Handhabung

Dieses Kapitel dient vorbereitend zur Identifikation möglicher Gefährdungen und deren Handhabung hinsichtlich BYOD im organisatorischen und technischen (Applikations- und Geräteebene) Bereich, wie in Kapitel 2.3 strukturiert.

3.1 Organisatorische Ebene

Der organisatorische Bereich umfasst die Regelungsmöglichkeiten, die durch die Mitarbeiter beeinflusst werden können.

3.1.1 Mitarbeiterkompetenz

Ein großes Problem im Zusammenhang mit BYOD stellen Anwender dar, die ein fehlendes Bewusstsein für die möglichen Sicherheitsgefahren in diesem Zusammenhang haben. Um diese Sensibilität zu fördern, sind beispielsweise *Schulungen* ein oft eingesetztes Mittel. In solchen *Awareness-Schulungen* kann beispielsweise der berufliche Umgang mit den privaten mobilen Geräten thematisiert und ein Verständnis für Sicherheitsvorkehrungen wie sichere Passwörter geschaffen werden [vgl. 27, S.179].

3.1.2 Social Engineering

Ein klassisches Beispiel für den zuvor angesprochenen „Sicherheitsfaktor Mensch“ ist *Social Engineering*. Unter diesem Begriff wird ein Angriffsszenario verstanden, bei dem es einem Angreifer auch bei intakten technischen Sicherheitsvorkehrungen gelingt, einen Angriff erfolgreich zu gestalten. Der Ansatz basiert auf der Manipulierbarkeit der Mitarbeiter, die durch gezielte Impulse dazu animiert werden, diesen Angriff zu realisieren. Während diese Gefährdung generell für Mitarbeiter von Institutionen besteht, so ist diese im Zusammenhang mit BYOD aufgrund der größeren

Einflussmöglichkeiten des Mitarbeiters auf das Gerät noch als verstärkt einzuordnen. *Social Engineering* findet beispielsweise oft im Zusammenhang mit *Phishing* statt. „Phishing beschreibt die Bedrohung, bei der ein Angreifer durch Nachahmung und Vortäuschung einer dem Nutzer bekannten Internetseite versucht, z. B. an dessen Zugangsdaten (z. B. Benutzerkennungen und Passwörter) oder Autorisierungstoken zu gelangen.“[35, S.148 f.] Der Kontakt erfolgt beispielsweise via E-Mail und fordert gegebenenfalls über eine gefälschte Internetseite zur Eingabe geheimer Daten auf. *Social Engineering* dient dazu, dieses Szenario mit persönlichen Angaben des Mitarbeiters zu hinterlegen, so dass dieses für den Mitarbeiter ein größeres Maß an Echtheit darstellt. Verhindern bzw. Abmildern lässt sich *Social Engineering* in allen Formen praktisch nur durch entsprechende Sensibilisierung des Mitarbeiters etwa durch die bereits angesprochenen *Awareness-Schulungen.*

3.1.3 Rechtliche Einschränkungen

Eine Absicherung der Geräte zum Schutze der institutionellen Informationen und zur Einhaltung rechtlicher Vorgaben bedeutet zumeist eine Einschränkung der Freiheiten des Mitarbeiters. Die aus rechtlicher Sicht notwendigen Regelungen bei BYOD können in einer Nutzungsvereinbarung getroffen werden, die vom Mitarbeiter vor Freischaltung für das Programm akzeptiert werden muss. Im Rahmen dieser Arbeit können juristische Aspekte nur in Ansätzen angesprochen werden. Für weitergehende Informationen sei auf entsprechende Literatur [35] verwiesen.

Eine Nutzungsvereinbarung, als rechtliche Absicherung, ist nach Monsch hinsichtlich BYOD in vier Arten denkbar: Direktionsrecht, Individualvereinbarung, Betriebsvereinbarung und Arbeitnehmer-Nutzungsrecht [vgl. 35, S.29ff]. Darauf basierend lässt sich festhalten, dass für die rechtssichere Einführung von BYOD eine arbeitsvertragliche Regelung oder eine Zusatzvereinbarung von Nöten ist. Sofern ein Betriebsrat existiert, können daraus resultierende Rechte und Pflichten auch in Form einer Betriebsvereinbarung fixiert werden.

Aus arbeitsrechtlicher Sicht sind nach Monsch auch einige Aspekte in der Nutzungsvereinbarung zu berücksichtigen [vgl. 35, S.44 ff.]:

- **Freiwilligkeit:** Unabhängig von der Form muss alleine schon aus datenschutzrechtlichen Gründen die Freiwilligkeit der Teilnahme betont werden. Dies begegnet zugleich dem Vorurteil, BYOD würde dazu führen, Arbeitgeberpflichten auf den Arbeitnehmer abzuwälzen.
- **Einschränkung der privaten Nutzung:** Da in der Privatnutzung ein hohes Gefahrenpotential liegt, stellt sich die Frage, ob dem Mitarbeiter eine gewisse Einschränkung während und außerhalb der Arbeitszeiten zumutbar wäre. Während eine Beschränkung der Privatnutzung während der Arbeitszeiten durchaus

für möglich und ggf. sinnvoll gehalten wird, so wäre ein Ausschluss der Privatnutzung außerhalb der Arbeitszeiten zwar theoretisch denkbar, würde aber das BYOD-Konzept ad absurdum führen. Gerade in der kombinierten privaten und betrieblichen Nutzung des Gerätes liegt ja die Stärke des BYOD-Programms. Eine teilweise Einschränkung der privaten Nutzung außerhalb der Arbeitszeiten wäre rechtlich zwar möglich, aber der Motivation zur Teilnahme am BYOD-Programm sicher nicht zuträglich. Grundsätzlich sollte die Einschränkung der privaten Nutzung immer nur dann in Erwägung gezogen werden, wenn triftige Sicherheitsaspekte dafür sprechen und keine andere Möglichkeit zur akzeptablen Gefährdungsreduktion besteht.

- **Arbeitszeitregelungen:** Da durch BYOD die zeitliche Abgrenzung zwischen Arbeits- und Freizeit verschwimmen, stellt sich in mehrfacher Sicht die Frage, wann der BYOD-Einsatz als Arbeitszeit gewertet werden muss. Laut einer Umfrage sind ein Drittel aller Beschäftigten auch außerhalb der regulären Arbeitszeit per Smartphone oder E-Mail für dienstliche Zwecke erreichbar [vgl. 5, S.28]. Zur Entscheidung, ob eine Tätigkeit arbeitszeitrechtlich relevant ist, soll an dieser Stelle ohne den Anspruch einer rechtlich vollständigen Betrachtung, eine kurze Einordnung vorgenommen werden. Für eine detaillierte, rechtlich einwandfreie Betrachtung, wird auf die entsprechende Fachliteratur verwiesen.

  - Da es sich bei BYOD um eine Zwischenform von Freizeit und Arbeitszeit handeln kann, wird von einer Form von *Bereitschaft* ausgegangen. Unterschieden werden die Kategorien *Arbeitsbereitschaft*, *Bereitschaftsdienst* und *Rufbereitschaft*. Auch wenn bei BYOD alle Formen dieser Bereitschaft auftreten können, so ist die *Rufbereitschaft* vermutlich die häufigste Variante. Sie zeichnet sich dadurch aus, dass sich der Arbeitnehmer dazu verpflichtet, jederzeit erreichbar zu sein. Er ist dabei in der Wahl seines Aufenthaltsortes frei, sofern er eine entsprechende Verfügbarkeit (Kommunikationsverbindung) sicherstellt. Sobald er eine Arbeitsleistung aufnimmt, wird diese Zeit in der Regel als Arbeitszeit berechnet.

  - Zusätzlich zur *Bereitschaft* ist weiter die Form der *Anordnung* von Bedeutung. Es wird hierbei unterschieden, ob der Arbeitgeber die Bereitschaft zur Erreichbarkeit anordnet bzw. dies unausgesprochen erwartet oder die Nutzung ohne ausdrückliche Anordnung stattfindet. Während bei Anordnung durch den Arbeitgeber eine Nutzung während der Arbeitszeit stattfindet, so will sich der Mitarbeiter im letztgenannten Fall lediglich „auf dem Laufenden halten“ und kann dies nicht der Arbeitszeit zuordnen.

  - Ist der BYOD-Einsatz der Arbeitszeit zuzurechnen, ist auf Einhaltung der maximalen täglichen Arbeitszeit zu achten. Auch die Verpflichtung zur Einhaltung der Ruhezeiten zwischen den Arbeitseinsätzen besteht

ungeachtet. Umstritten ist allerdings, ob auch eine *geringfügige Unterbrechung* etwa durch kurzes Beantworten einer E-Mail eine *nennenswerte Arbeitsleistung* darstellt und damit die Ruhezeit stört. Wäre dies der Fall, könnte BYOD nur sehr eingeschränkt betrieben werden.
Diese Problematik gilt auch für den Einsatz an Sonn- und Feiertagen. Hier darf der Arbeitgeber nach gängiger Rechtsauffassung eine BYOD-Tätigkeit nicht nur nicht annehmen, er darf sie weder zulassen noch dulden, sondern muss diese aktiv verhindern.

Hinsichtlich der Gesetzeslage ist vor allem das Telekommunikations- und das Datenschutzrecht von Bedeutung:

- Das **Telekommunikationsgesetz (TKG)**[1] regelt vor allem die Fragestellung wann der Arbeitgeber als Diensteanbieter für die private Nutzung des BYOD-Gerätes gilt. Diese Frage ist nicht pauschal zu beantworten und hängt auch damit zusammen, welcher Netzzugang durch den Mitarbeiter genutzt wird. Grundsätzlich gilt bei privater Nutzung einer (dienstlichen) SIM-Karte oder der betrieblichen Internetsysteme (WLAN-Netz der Institution) jedoch: „dass ein Arbeitgeber, der seinen Arbeitnehmern die private Nutzung der betrieblichen Telekommunikationsmöglichkeiten gestattet, mit der herrschenden Ansicht in der Literatur als Diensteanbieter i. S. des § 3 Nr. 6 TKG dem einfachgesetzlichen Fernmeldegeheimnis unterfällt.“[35, S.121] Monsch empfiehlt deshalb die Lösung „in umfassenden technischen Vorkehrungen und eindeutigen Nutzungsbestimmungen zu suchen.“[35, S.121]
  Für weitergehende Informationen sei auf Monsch[35, S.110 ff.] verwiesen.

- Da auf den BYOD-Endgeräten personenbezogene Daten im Sinne des Art. 4 Abs. 1 Nr. 1 DSGVO[2] verarbeitet werden, greift (unabhängig von der Geltung des Telekommunikationsgesetzes (TKG)) das **Datenschutzrecht**. Die zentrale Frage im Zusammenhang mit BYOD ist hier, ob der BYOD-Einsatz „zur Anwendung der Vorschriften der Auftragsdatenverarbeitung führt, wenn Arbeitnehmer personenbezogene Daten auf ihren privaten Endgeräten verarbeiten oder nutzen.“[35, S.131] Diese Frage wird kontrovers diskutiert[vgl. 35, S.132 f.] und lässt sich nicht eindeutig beantworten. Die Tendenz geht aber dahin, dass kein Vertrag zur Auftragsdatenverarbeitung abgeschlossen werden muss, da der BYOD-Nutzer die personenbezogenen Daten weiterhin als Mitarbeiter der Institution verarbeitet. Die Institution hat jedoch als verantwortliche Stelle gemäß Art. 24 Abs. 1 Nr. 1 DSGVO[3] dafür Sorge zu tragen, dass geeignete technische und organisatorische Maßnahmen zum Einsatz kommen um die

[1] `https://www.gesetze-im-internet.de/tkg_2004/`
[2] `https://dsgvo-gesetz.de/art-4-dsgvo/`
[3] `https://dsgvo-gesetz.de/art-24-dsgvo/`

datenschutzrechtlichen Vorschriften zu erfüllen.
Für weitergehende Informationen sei auf Monsch[35, S.129 ff.] verwiesen.

Zusammenfassend lässt sich festhalten, dass der BYOD-Einsatz aufgrund vielfältiger rechtlicher Fallstricke zwingend einer Nutzungsregelung bedarf [vgl. 35, S.129].
In der Nutzungsregelung sollte geklärt werden, ob und wenn ja in welcher Weise der Arbeitgeber die Erreichbarkeit außerhalb der vereinbarten Arbeitszeit erwartet. Ohne tiefere Betrachtung der arbeitsrechtlichen Situation sollte dies nicht erfolgen, sondern besser auf jegliche Verpflichtung verzichtet werden, so dass der Arbeitnehmer BYOD als Informationsmöglichkeit auf freiwilliger Basis anerkennt. Ebenfalls problematisch ist die Verpflichtung des Arbeitgebers ein Nutzungsverbot an Sonn- und Feiertagen durchzusetzen. Dies kann nur durch temporäre Deaktivierung der Dienste auf technischer Ebene realisiert werden.
Des weiteren zu empfehlen ist unter anderem die Beachtung des Telekommunikationsgesetzes (TKG) und der Datenschutzgrundverordnung (DSGVO). Auch wenn das TKG nur unter bestimmten Umständen greift, so gelten auf jeden Fall die Bestimmungen der DSGVO. Technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten müssen in dem Umfang eingesetzt werden, dass „ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.“[35, S.134]

3.2 Technisch auf Applikations- und Geräteebene

Im technischen Bereich liegt der Fokus auf Gefährdungen, die zumeist durch äußere Einflüsse initiiert werden. Die Auswirkungen und daraus resultierenden Handhabungsmöglichkeiten variieren je nach eingesetzten Endgeräten. Hier werden in kompakter Darstellung einige ausgewählte Faktoren untersucht und Lösungsansätze genannt.

3.2.1 Schadsoftware

Unter Schadsoftware fallen alle Programme, die einem System Schaden zufügen können. Dies sind im Detail Viren, Trojaner, Würmer und ähnliche. Die Schäden, die diese Programme auslösen können, sind vielfältig: Beispielsweise Nutzung des Systems für weitere Angriffe (Botnet) oder Ausspähen von Zugangsdaten. Unabhängig von BYOD sind von dieser Bedrohung natürlich auch lokale IT-Systeme betroffen. Bei smarten Endgeräten erhöht sich dieses Risiko jedoch durch weitere Faktoren [vgl. 27, S.146]:

- Smartphones und Tablets werden rund um die Uhr betrieben

- Smartphones und Tablets haben rund um die Uhr Internetkonnektivität
- Nutzer akzeptieren häufig gutgläubig selbst weitreichende Berechtigungsanforderungen von Applikationen
- Applikationen auf Smartphones und Tablets können im Hintergrund aktiv werden bzw. bleiben.
- Smartphones und Tablets eignen sich aufgrund der integrierten Mikrofone und Kameras auch als Wanzen.

Zusätzlich tragen die umfangreicheren Rechte, die ein Nutzer auf seinem eigenen Geräte in der Regel hat und der Betrieb außerhalb der Institution dazu bei, das Risiko für Schadsoftware zu erhöhen.
Hinsichtlich der Anfälligkeit für Schadsoftware unterscheiden sich die verbreiteten Betriebssysteme aufgrund ihres Konzepts. Versionen für Desktop-Computer bzw. Laptops wie Windows 10 oder macOS sind individueller konfigurierbar und durch ihre Schnittstellen vielfältiger zu erweitern als ihre mobilen Pendants auf Smartphones oder Laptops. Zusätzlich bringt echte Multitasking-Fähigkeit[4] ein weiteres Risiko von im Hintergrund laufender Schadsoftware mit sich. Dadurch wird auch der Schutz schwieriger und zusätzliche Maßnahmen in Form von spezieller Software (Firewall, Antivirus, Malware etc.) sollten zum Einsatz kommen.
Die Erweiterbarkeit durch Drittanbieter-Programme ist ein weiterer Unterschied zwischen herkömmlichen Betriebssystemen und den Varianten auf smarten Mobilgeräten. Während beim traditionellen System die Wahl aus einem umfangreichen, freien Softwareangebot unterschiedlicher Quellen (Internet, Datenträger etc.) erfolgt, so sind Android und iOS auf so genannte App-Stores als Lieferanten begrenzt. Android kann wahlweise auch Apps aus freien App-Stores laden, iOS nur aus dem Apple-eigenen Store. Gerade letztgenannte Variante bringt eine erhöhte Sicherheit mit sich, da nur getestete Software auf die Systeme gelangt. „Zwar prüft auch Google jede App vor deren Einstellung in den Google Play Store hinsichtlich einiger inhaltlicher Aspekte sowie der Einhaltung von Googles Programmrichtlinien, jedoch gehen die Anforderungen und Kontrollen hierbei nicht so weit, wie z.B. die bei Apple für deren iTunes Store.“[27, S.147] Die Android-Plattform ist aber laut Kohne et al. nicht nur aus diesem Grund gefährdeter für Schadsoftware: Die deutlich größere Verbreitung (siehe Kapitel 4.3) steigert die Attraktivität zur Entwicklung von Schadsoftware für diese Plattform und die Update-Politik variiert je nach Hersteller, so dass neue Firmware-Versionen oft erst mit Verzögerung zur Verfügung stehen [vgl. 27, S.147].

> „Da bei iOS-Geräten sowohl Hardware als auch Software ausschließlich von Apple kommt, werden neue Betriebssystem-Versionen stets für alle

[4] Ausführen mehrerer Programme parallel, zum gleichen Zeitpunkt.

> Geräte gleichzeitig verfügbar gemacht. Ältere Geräte werden in der Regel über mehrere Jahre unterstützt, und zwar solange wie die Hardware-Ausstattung noch von Apple als ausreichend für die jeweils nächste Betriebssystem-Version erachtet wird.“ [27, S.147]

Google hat sich mit neueren Versionen von Android hinsichtlich der Sicherheit an vielen Punkten verbessert (siehe auch Kap.4.3), aber trotzdem sind diese Nachteile aus früheren Zeiten bei einigen Entscheidungsträgern noch präsent und führen dazu, dass man die Android-basierten Geräte beim BYOD-Programm nicht oder nicht im vollen Umfang unterstützt (siehe dazu auch Kap. 2.4).
Bei Installationen jeglicher Art muss in der Regel das Gerätekennwort bzw. ein Passwort eines berechtigten Accounts zur Bestätigung eingegeben werden. Dies stellt einen weiteren Schutzmechanismus gegen ungewünschte Installationen dar und wird bei Windows in den aktuellen Versionen und macOS auch standardmäßig eingesetzt.
Ein weiterer Unterschied zwischen Desktop-Betriebssystemen und Betriebssystemen für smarte Geräte ist außerdem die Verbindung zu der Hardware, auf der sie läuft. Gerade Desktop-Computer aber auch Laptops können in verschiedener Weise hardwaretechnisch aufgerüstet und damit verändert werden. Dieses bewusste Vorgehen stellt die Anforderung an das Betriebssystem, sich anzupassen. In der Regel geschieht diese Anpassung durch die Installation von Treiber-Software, die mittels definierter Schnittstellen tiefergehenden Zugriff in das System erhalten. Um ein Einschleusen von Schadsoftware auf diesem Wege zu verhindern, werden oftmals nur noch signierte Treiber zugelassen. Diese wurden zuvor vom Hersteller des Betriebssystems zertifiziert und werden dann zu Beginn der Installation daraufhin geprüft, ob die Software der ursprünglich eingereichten Version entspricht. Der Nutzer kann die Einschränkung auf signierte Treiber manuell aufheben[5]. Diese Deaktivierung sollte aus sicherheitstechnischer Sicht unterlassen werden.
Aber nicht nur das Betriebssystem ist ein potentielles Ziel für Schadsoftware, sondern auch das darunter liegende Startsystem für das initiale Ansprechen der Komponenten. Früher wurde diese Aufgabe vom *BIOS*[6] übernommen. Bei neueren Rechnergenerationen ist dafür nun das so genannte *UEFI*[7] zuständig. Während Mac-Rechner schon seit dem Jahr 2006 auf diese Schnittstelle setzen, sind bei Windows-basierten Systemen erst seit ca. 2010 Mainboards mit *UEFI* verfügbar. Sicherheitstechnischer Vorteil von *UEFI* ist der so genannte Secure-Boot-Mechanismus, der sicherstellt, dass nur signierte Bootloader genutzt werden können, womit es Schadsoftware auch zu diesem Zeitpunkt des Systemstarts erschwert wird, geladen zu werden. Damit

[5] `https://www.deskmodder.de/wiki/index.php/Treibersignatur_deaktivieren_Unsignierte_Treiber_installieren_Windows_10`

[6] Abkürzung für „basic input/output system“. Nichtflüchtiger Speicher mit der initialen Firmware zum Ansprechen der einzelnen Komponenten des Computers.

[7] Abkürzung für „Unified Extensible Firmware Interface“. Zentrale Schnittstelle zwischen Firmware, Hardware und Betriebssystem eines Computers.

soll eine vertrauenswürdige Abfolge von der Firmware über den Systemstart bis zur Benutzeranwendung sichergestellt werden. Um auch bei neu auftretenden Sicherheitsproblemen im Zusammenhang mit *UEFI* angemessen reagieren zu können, wurde eigens eine Anlaufstelle in Form des *UEFI Security Response Team (USRT)*[8] geschaffen. Dieser Kontakt reagiert auf gemeldete Sicherheitsvorfälle, prüft sie und leitet sie ggf. an die richtige Stelle bzw. den passenden Hardwarehersteller weiter.
Eine neuere Entwicklung in dieser Richtung stellen spezielle Sicherheitschips dar, die als Coprozessor diverse Systemvorgänge absichern [vgl. 3].

Auch wenn sie noch keine große Verbreitung haben, so lässt sich feststellen, dass durch den Einsatz eines Sicherheitschips wie des Apple T2 das Sicherheitsniveau eines IT-Systems zusätzlich erhöht werden kann. Apple Mobilgeräte verfügen ebenfalls über Sicherheitskomponenten, die neben Aufgaben wie der Datenverschlüsselung (siehe Kap. 2.3.7) auch das Herstellen einer vertrauenswürdigen Bootkette (Secure boot chain) realisieren. Ausgehend vom read-only Speicher (Boot Rom), welches auch als „root of trust“ bezeichnet wird, wird anhand einer Kette von Signaturen die Integrität der zu ladenden Daten sichergestellt: „This is the first step in the chain of trust where each step ensures that the next is signed by Apple.“[1, S.6]
Android hat in bestimmten Varianten (etwa bei BlackBerry, siehe Kapitel 2.3.7) ähnliche Sicherheitsmechanismen implementiert.

3.2.2 Diebstahl und Verlust

Desto kompakter, leichter und damit transportabler ein Endgerät ist, desto größer ist das Risiko, dass es verloren geht oder unbemerkt entwendet wird. Dies gilt vor allem für Smartphones, die oftmals in der Kleidung mitgeführt werden. Einer Studie [vgl. 27, S.138] nach bemerken es nur 21% der Betroffenen unmittelbar wenn sie das Smartphone verlieren bzw. es ihnen entwendet wird. Dies stellt vor allem in Kombination mit fehlendem oder unzureichendem Zugriffsschutz und/oder fehlender Datenverschlüsselung eine Gefahr dar.
Im *Mobile Theft & Loss Report* wurde von der Firma *Prey*[9], dem Anbieter einer OpenSource Lösung zur Ortung und Ergreifung von Sicherheitsmaßnahmen, anhand der Kundenrückmeldungen realer Fälle eine Untersuchung bzgl. Diebstahl bzw. Verlust von Endgeräten durchgeführt [vgl. 38]. Die wichtigsten Ergebnisse dazu:

- Es wurde initial festgestellt, dass fast 70% der Verluste auf einfaches Verlegen zurückzuführen sind. Erst danach folgen Diebstahl mit ca. 11%, Einbruch mit 8% sowie Raub mit 7% [38, S.7].

[8] `https://uefi.org/security`
[9] `https://preyproject.com`

- Ein Verlegen passiert zumeist zu Hause (28%) und ein Entwenden ebenso häufig in öffentlichen Verkehrsmitteln (28%) [38, S.8].

- 63% der Vorfälle finden an gesicherten Orten (Zu Hause, Büro, Schule/Uni oder Auto) statt. Nur 37% an ungesicherten, öffentlichen Orten [38, S.15].

Zudem bemerkten einer Studie von Absolute Software zufolge nur 21% der Befragten, die bereits einmal ihr Mobiltelefon verloren haben, den Verlust unmittelbar. 55% registrierten diesen erst innerhalb von 4 Stunden und bei 24% dauerte es gar noch länger.[vgl. 44]

Um Diebstahl und Verlust vorzubeugen, empfehlen sich sowohl *proaktive* als auch *reaktive* Maßnahmen wie beispielsweise:

- **Proaktiv**

  - **Zugriffsschutz:** Dies lässt sich entweder per PIN-Code oder via biometrischer Eingabe (z.B. Fingerabdruck, Gesichtserkennung, Iris-Scanner oder Venenscanner) realisieren. Bei der Einstellung des PIN-Codes sollte mindestens die längere Variante (6-stellig) benutzt werden. Auf die früher verbreitete Form der „Wischmuster“ (Unlock-Patterns) bei Android sollte verzichtet werden, da die Muster bestimmten Regeln folgen und damit nicht die gewünschte Sicherheit bieten. So wurde beispielsweise festgestellt, dass Muster oftmals am oberen linken Eckpunkt starten und damit die Anzahl möglicher Eingaben schon deutlich reduziert wird [vgl. 31, S.108]. Oftmals verraten auch schon Fingerspuren auf dem Display das Muster.
    Interessant ist in diesem Zusammenhang auch die Betrachtung der plattformabhängigen Qualität des Zugriffsschutz zwischen klassischen Betriebssystemen und den „smarten“ Pendants. Während bei Windows oder macOS das Passwort in Form eines Freitexts festgelegt werden kann, so ist bei Android oder iOS in der Regel die Eingabe einer Zahlenkombination (PIN) üblich [vgl. 51, S.83].
    Die Absicherung mittels Passwörtern bzw. PIN ist auch nach Kölbel das Mittel der Wahl: „Obwohl nachgewiesenermaßen Passwörter entweder so trivial sind, dass sie sich erraten lassen, oder zuhauf gestohlen werden, sind sie immer noch ein weit verbreitetes Verfahren im Bereich Identitäts- und Zugriffsmanagement.“[29, S.38] Auch bei Verwendung komplizierterer Passwörter kann es durch Nutzung des gleichen Passworts an anderer Stelle ein Sicherheitsrisiko geben: „The major hack of Yahoo! provides the perfect example of this after hackers stole over a billion usernames and passwords. While this was more down to poor cyber-security from the technology giant, if people are using similar passwords then it can increase the risk of further systems being compromised.“[46, S.7] In neueren

Geräten wird die Authentifizierung auch mittels biometrischer Verfahren, wie etwa Fingerabdruck oder Gesichtsscanner ermöglicht: „While the technology is still fairly new, more and more organisations will see its benefits, making it commonplace across SMEs'[10] BYOD policies in the future."[46, S.7] Zu Grunde liegend existiert aber auch bei der Nutzung biometrischer Verfahren in der Regel nach wie vor ein Passwort oder eine PIN als alternative Eingabemöglichkeit.
Als zusätzliche, praxistaugliche Maßnahme zur Erhöhung der Sicherheit empfiehlt Kölbel „die *Zwei-Faktor-Authentifizierung*, deren Einführung die Zugangssicherheit deutlich erhöhen kann."[29, S.38] Bei diesem Verfahren wird zusätzlich zur PIN-Eingabe eine weitere, davon unabhängige Eingabe, benötigt. Dies kann beispielsweise ein temporärer Code sein, der auf ein anderes (als vertrauenswürdig eingestuftes) Gerät geschickt wird. Aber auch eine kombinierte Eingabe von Fingerabdruck und PIN fällt unter dieses Verfahren.

- **Datenverschlüsselung:** Um die gespeicherten Daten bei einem Geräteverlust zu schützen, sollten die Daten auf dem Gerät, wie in Kapitel 2.3.7 bereits dargestellt, verschlüsselt werden.

- **Vorsichtsmaßnahmen:** Vorbeugen durch bestimmte Verhaltensmaßnahmen wie beispielsweise das Handy nicht in die Gesäßtasche stecken oder das Tablet nicht offen im Auto liegen lassen, kann das Risiko eines Verlusts senken.

- **Technische Hilfsmittel:** Gegen Verlust eines Smartphones oder Tablets gibt es auch technische Gadgets (beispielsweise *Tile*[11]), die nach einmaliger Kopplung dann einen Alarm auslösen, wenn sich das Gerät zu weit von diesem entfernt.

- **Reaktiv**

  - **Ortung/Sperrung/Löschung:** Dienste zur Ortung nutzen die GPS-Funktion des Gerätes (sofern verfügbar) und/oder die etwas ungenauere Angabe über eine Internetverbindung. Eine funktionierende Internetverbindung ist jedoch Voraussetzung zur Aktualisierung der Standortdaten[12]. Wenn das Gerät geortet werden kann, so können aus der Ferne weitere Aktionen wie beispielsweise eine Sperrung oder komplette Löschung durchgeführt werden.

[10] Small and medium-size enterprises
[11] `https://www.thetileapp.com/de-de/`
[12] Es gibt aktuell Entwicklungen, mittels eines sogenannten „Find-Networks" Datenverbindungen alternativ über in der Nähe befindliche Geräte herstellen zu können (vgl. dazu: `https://9to5mac.com/2019/04/17/find-my-iphone-revamp/`).

Die verbreiteten Desktop-Betriebssysteme Microsoft Windows, macOS, Android oder iOS bieten in ihren aktuellen Versionen von Hause aus Funktionen zur Ortung/Sperrung an. Diese müssen lediglich aktiviert und durch Anmeldung bei Microsoft (Live-Account)[13], Apple (iCloud)[14] oder Google[15] in der Regel kostenlos mit einem Online-Konto verknüpft werden.
Mit dem bereits erwähnten *Prey* gibt es überdies beispielsweise auch plattformübergreifende Lösungen, die zudem eine Unternehmensverwaltung unterstützen.

3.2.3 Elementareinflüsse

Mobile Geräte sind aufgrund ihrer ortsunabhängigen Nutzbarkeit auch Gefährdungen ausgesetzt, die auf stationäre Geräte nicht in diesem Maße zutreffen. Während beispielsweise Smartphones einen Regenschauer in der Hosentasche in der Regel schadlos überstehen, so kann der klassische freie Fall aus eben dieser auf einen harten Untergrund einen Schaden herbeiführen, der das Gerät unbenutzbar machen und folglich die Verfügbarkeit gefährden kann. Folgende Elementareinflüsse können auf diese Geräte einwirken:

- **Wasser:** Feuchtigkeit und Wasser können elektrische Geräte beschädigen. Dieses Szenario tritt relativ oft auf, so dass einige Hersteller zur eigenen Absicherung sogar Indikatoren in mobilen Geräten verbauen[16]. Diese verfärben sich dauerhaft wenn Feuchtigkeit an sie gelangt. Resistent gegen Wasser oder zumindest Spritzwasser sind immer noch nur wenige Geräte. Der Aufwand zur Abdichtung von Anschlüssen und Knöpfen ist relativ hoch und aufwändig. Trotzdem gibt es solche Geräte oder zumindest bei Smartphones wasserdichte Schutzgehäuse.

- **Feuer:** Gegen Feuer sind elektronische Geräte nahezu wehrlos. Die verbauten Kunststoffe und die Akkus sind sehr hitzeempfindlich. Auch die gespeicherten Daten sind durch Feuer hochgradig gefährdet. Während Festspeicherplatten (SSD)[17] viele Vorteile haben, so ist eine Rekonstruktion nach Brandschäden noch schwieriger als dies bei klassischen Magnetfestplatten der Fall ist. Dies liegt an einem proprietären Verfahren namens Wear-Leveling, wobei die Daten

[13] `https://support.microsoft.com/de-de/help/11579/microsoft-account-find-and-lock-lost-windows-device`
[14] `https://www.apple.com/de/icloud/find-my-iphone/`
[15] `https://support.google.com/accounts/answer/6160491?hl=de`
[16] https://support.apple.com/en-us/HT204104
[17] Abkürzung für Solid State Drive. Auf Flash-Speicher basierender Datenspeicher ohne mechanisch bewegte Teile.

vom Flash-Controller auf die Flash-Speicher verteilt werden, teilweise sogar verschlüsselt [vgl. 23]. Bei Magnetfestplatten ist eine Rekonstruktion auch ohne funktionierende Technik durch (partielles) Auslesen der Speicherplatten möglich.

- **Blitz:** Blitze können zu Überspannungen im Stromnetz führen. Diese Gefährdung betrifft vor allem Desktop-Computer. Während in Institutionen möglicherweise Netzfilter oder USVs[18] die Stromversorgung absichern, ist dies im Privathaushalt oftmals nicht der Fall. Dadurch sind die Netzteile diesen Spannungsspitzen ungeschützt ausgesetzt. Auch andere elektronische Komponenten sind gefährdet: „Überspannungsschäden zerstören Flash-Chips, wo bei Magnetfestplatten vielleicht nur der Controller ausfällt, nicht aber die Magnetscheibe.“ [23] Bei mobilen Geräten ist diese Gefährdung dank der autarken Akku-Funktion stark reduziert. Nur durch das Laden am Netzteil kann ein Schaden auftreten. Am stärksten gefährdet wäre aber das Netzteil selber. Dies würde jedoch nicht zwangsweise zu einem Ausfall des Gesamtsystems führen.
- **Erschütterungen:** Im vertretbarem Maße sind mobile Geräte gegen Erschütterungen gut geschützt. Die empfindlichste Komponente war immer die Magnetfestplatte, die heutzutage gerade im Bereich der Laptops und Smart-Devices nahezu vollständig gegen Festspeicherplatten (SSD) ersetzt worden sind. Diese sind ohne bewegliche Komponenten deutlich robuster gegen Erschütterungen.
- **Fall:** Desto kompakter mobile Geräte sind, desto größer ist die Gefahr, dass diese dem Benutzer auch mal aus der Hand rutschen. Die meisten Consumer-Geräte haben keine besonderen Vorkehrungen Stürze dieser Art abzufangen. Für die empfindlichen Touch-Screens gibt es zwar speziell gehärtetes Glas (beispielsweise unter der Bezeichnung *Gorilla*), dieses kann gesprungene Displays aber auch nur bis zu einer bestimmten Belastung verhindern. Der Schutz kann zusätzlich durch spezielle Hüllen, die das Gerät äußerlich ummanteln, erhöht werden.

Smartphones und Tablets können mit zusätzlichen Sicherheitsmaßnahmen (Schutzcases) etwas besser gegen einige der oben genannten Elementareinflüsse geschützt werden. Ein vollumfänglicher Schutz lässt sich jedoch auch auf diese Weise nicht erreichen. Ähnlich gut geschützte Geräte bereits ab Werk, gibt es unter dem Begriff *Ruggedized*, welche zumeist auf Android basieren.

[18] Unterbrechungsfreie Stromversorgung mittels Akku zur Überbrückung von Stromausfällen

4 Smart Devices im Unternehmensumfeld

Dieses Kapitel legt den Schwerpunkt auf die so genannten *Smart Devices*[1] mit Blick auf den Unternehmenseinsatz. Diese verwenden ein spezielles Betriebssystem, können eine Verbindung zum Internet herstellen und werden in der Regel nicht vollständig ausgeschaltet. Auf die Frage, wie sich diese von klassischen PCs weiter differenzieren, empfehlen Lugtig und Toepoel: „In our view, all devices can be classified along two dimensions: (1) screen size and (2) method of data entry."[30, S.79] Dieser Vorschlag ist nachvollziehbar, da es sich bei Bildschirmgröße und Eingabemöglichkeit um die primären Schnittstellen zum Benutzer handelt.

4.1 Anwendungsgebiete

„Smarte" Geräte übernehmen im Alltag zunehmend Aufgaben klassischer IT-Geräte. Während im Jahr 2015 noch Desktop PCs mit 62,4% den höchsten Marktanteil hatten (Smartphone 31,1% und Tablet 6,5%), so haben Smartphones diese mittlerweile abgelöst. Mit Stand März 2019 haben Smartphones einen Marktanteil von 49,07% und Tablets von 3,98%, während Desktops noch einen Anteil von 46,94% ausmachen.[2] Dies zeigt, dass mobile Geräte sowohl im geschäftlichen als auch privaten Bereich mehr und mehr an Bedeutung gewinnen.
Eine der Hauptanwendung für mobile Geräte liegt in der Nutzung von sogenannten *PIM*[3]-Funktionen wie E-Mails, Kalender, Kontakte und Aufgaben. Abseits dieser Basisaufgaben sind heute noch viele andere Funktionalitäten denkbar. Es ist jedoch zu beachten, dass diese Geräte gemäß der Klassifikation von Lugtig und Toepoel anhand von Bildschirmgröße und Eingabemöglichkeit gegenüber klassischen Computern beschränkt sind [vgl. 30, S.79]. Komplexe Aufgaben sind schwieriger zu realisieren. Dies bestätigt auch eine Studie von de Bruijne und Wijnant, die anhand einer Umfrage untersucht haben, in welcher Weise sich die Nutzung von Smartphones, Tablets und

[1] Unter diese Klasse fallen neuere Gerätetypen wie unter anderem Smartphones, Tablets oder auch Wearables.
[2] `http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide`
[3] Personal Information Manager

klassischen PCs unterscheidet. Hinsichtlich der Effizienz stellten de Bruijne und Wijnant fest: „We found that respondents using a mobile device evaluated the survey to last longer than respondents using a computer.“[16, S.494] Die Gründe für diese Feststellung vermuten die Autoren in der Schnittstelle zum Nutzer, wobei ein zusätzlicher Einfluss von technischen Faktoren nicht ausgeschlossen werden kann: „This implies that the mobile survey still requires more effort from the respondent, which could be due to lower page loading speed, slower Internet connection, or more difficult task handling.“[16, S.494] Diese Annahme wird davon gestützt, dass wiederum kein signifikanter Unterschied hinsichtlich der Effizienz zwischen Tablet- und PC-Benutzung festgestellt werden konnte. de Bruijne und Wijnant betonen, dass viele Untersuchungen die Schwierigkeiten auch auf die kleinere Bildschirmgröße der Geräte zurückführen[vgl. 16, S.494] und konnten feststellen, dass eine Vereinfachung der Darstellung durch kürzere Texte und Anpassungen die Probleme beseitigt: „Accordingly, when the layout was adjusted to suit mobile browsers and the length of the question text was deliberately restricted, no major difficulties on the newer mobile devices were experienced in this respect.“[16, S.494] Eine an mobile Geräte angepasste Darstellung ist vor allem durch spezielle Programme, so genannte Apps realisierbar. Sie haben zudem den Vorteil die Hardware wie Kamera und Mikrofon nutzen zu können und somit auch AR[4]-Anwendungen zu ermöglichen, mit dessen Hilfe beispielsweise in der Planung von Einrichtungen Visualisierungen vorgenommen werden oder Reparaturen visuell unterstützt werden können.
Apps können in der Regel nicht mehr klassisch vom Datenträger installiert werden, sondern müssen aus einem der, für das entsprechende Betriebssystem angebotenen, App-Stores stammen. Das generelle Prinzip des App-Stores wird noch in Kapitel 4.3 behandelt. An dieser Stelle sei aber bereits erwähnt, dass es für die beiden großen Distributionen Android und iOS für Unternehmen auch eigene Company-/Enterprise-Stores gibt, über die die verbundenen Nutzer dann für sie ausgewählte Apps beziehen können.

4.2 Gerätetypen

Hinsichtlich der Gerätetypen kommen derzeit primär zwei Kategorien zum Einsatz:

- **Smartphones**
- **Tablets**

[4] Abkürzung für Augmented Reality. Beschreibt eine Funktion um das reale (Kamera)Bild mit einem virtuellen Objekt zu verknüpfen.

Zusätzlich gibt es mit **Phablets** und **Wearables** weitere Geräteklassen.

Smartphones haben sich in der heutigen Gesellschaft durch nahezu alle Altersschichten zum täglichen Begleiter entwickelt. Im Unternehmenssektor halten aufgrund von Sicherheitsbedenken schnelle technische Entwicklungen nicht immer unmittelbar Einzug. Zu groß ist die Angst durch Änderungen bestehende Abläufe und Prozesse negativ zu beeinflussen. Zudem genügten die Funktionalitäten der Geräte erst mit zunehmender Entwicklung der Betriebssysteme den Anforderungen um in den Informationsverbund des Unternehmens integriert zu werden. Das neben der reinen Aufnahme auch eine Anpassung der Prozesse notwendig ist, beschreiben Quade und Leimstoll in ihrer Untersuchung:

> „The descriptive analysis of the sample revealed that in most cases companies support only few of their business processes with smartphones and tablets. Nevertheless, most companies use unstructured information for their mobile work. Storing and accessing document-based information on a smartphone or tablet is easy and quickly done. In contrast, implementing process support on smartphones and tablets is much more challenging, because it needs specialist applications and an integration of the smart devices into the work processes. To fully explore the improvements in productivity and flexibility, processes often have to be redesigned according to the potential advantages provided by those devices.“ [40, S.300]

In diesem Zusammenhang sollte zusätzlich auch die Bereitschaft der potentiellen BYOD-Nutzer mit in Betrachtung gezogen werden. Nach den Daten einer Deloitte-Studie zur Nutzung von Smartphones [vgl. 20], werfen nach Feierabend gerade mal 13 Prozent der befragten Nutzer öfter mal einen beruflichen Blick auf ihr Smartphone. 38 Prozent machen dies nur ab und zu und knapp die Hälfte der Befragten tut dies nie. Die Anwendungsgebiete sind primär Kommunikation und Kalender. Anspruchsvollere Business-Anwendungen sind nicht sonderlich verbreitet.
Das Smartphones eher für einfache Aufgaben genutzt werden, bestätigen auch die Ergebnisse einer weiteren Untersuchung von Bröhl et al.: „With regard to the activities it was found that participants primarily use their smartphone for short message services, the tablet PC is primarily used for watching videos, the desktop PC is primarily used to write e-mails, (. . .).“[8, S.17]
Die Ergebnisse dieser Studien belegen, dass das Potential, dass Smartphones für den Einsatz im Business-Bereich haben, nicht alleine durch die Integration von Smartphones in den Informationsverbund einer Institution ausgeschöpft werden kann. Vielmehr bedarf es zusätzlich einer Anpassung der Prozesse und den Einsatz angepasster Software/Apps.

Für bestimmte Anwendungen gab es Bedarf für eine weitere Geräteklasse zwischen

Smartphone und Laptop: *Tablets* erbten viele Komponenten sowie das Betriebssystem zu großen Teilen vom Smartphone, differenzierten sich aber, gemäß der Kategorisierung von Lugtig und Toepoel, vor allem durch einen größeren Bildschirm und einer optionalen Eingabemöglichkeit mittels Stift [vgl. 30, S.79]. Dadurch wurde es möglich wie mit einem digitalen Notizblock zu arbeiten: Texte auf einer DINA4-ähnlichen Größe ansehen und Notizen handschriftlich direkt auf dem Display durchzuführen.
Im betrieblichen Umfeld hat die Nutzung von Tablets ebenfalls stark zugelegt. In einer Studie, die von Dynamic Markets zusammen mit Panasonic in 9 Ländern der EU durchgeführt wurde, konnte Folgendes festgestellt werden [vgl. 18]:

- 64% der deutschen Arbeitgeber empfinden eine substantielle Produktivitätsverbesserung bei ihren Mitarbeitern durch den Einsatz von Tablets
- 27% Produktivitätszuwachs stellen deutsche Arbeitgeber durch den Einsatz von Tablets fest
- 84% der Arbeitgeber mussten in den letzten zwei Jahren Probleme mit den Tablets in der Organisation feststellen
- 60% der deutschen Nutzer waren mit der Leistung ihres Tablets bei der Arbeit nicht vollständig zufrieden

Diese Ergebnisse belegen die grundsätzliche Bereitschaft und Überzeugung der Unternehmen Tablets produktivitätssteigernd einzusetzen. Auf der anderen Seite zeigen die Daten in Analogie zum Smartphone aber auch, dass die Integration in der Praxis noch verbesserungswürdig ist. Basierend auf den Verkaufszahlen, kommt Brandt in einer Analyse ergänzend dazu zum Ergebnis, dass Tablets ein Auslaufmodell seien:„In fact, the tablet hype seems to be over already with both IDC and Gartner revising their sales forecasts for this year, predicting a downward trend.“[6] Die Gründe dafür sieht Brandt vor allem in den fehlenden Anwendungsszenarien: „Additionally many people see little use for tablets in their everyday lives.“[6]
Vor dem Hintergrund sinkender Verkaufszahlen von Tablets[vgl. 6], sieht Brandt vor allem **Phablets**[5] als neuen „rising star“[6].
Auf der anderen Seite der Smartphones etablieren sich die so genannten Wearables derzeit vor allem in Form von *Smartwatches*, welche mittlerweile die technischen Möglichkeiten besitzen, bestimmte Funktionen der Smartphones zu übernehmen. Dies sind beispielsweise Authentifizierungsaufgaben wie Zutritts-/Zugangsfunktionen[6] oder Bezahldienste[7][8].
Im industriellen Umfeld werden auch zunehmend *smarte Brillen* genutzt, die beispielsweise Produktionsschritte direkt im Sichtfeld visualisieren oder überwachen

[5] Kategorie von mobilen Geräten zwischen der Größe eines Smartphones und der eines Tablets.
[6] `https://support.apple.com/de-de/HT206995`
[7] `https://www.apple.com/de/apple-pay/`
[8] `https://pay.google.com/intl/de_de/about/`

können. Mit diesen Brillen wird auch die Technologie *Augmented Reality*, der Kombination realer und virtueller Bilder, praxistauglich. Ansätze für Smarte Brillen gibt es schon seit 2013, ein nennenswerter Markt wird aber erst für ca. 2023 erwartet [vgl. 32].

4.3 Betriebssysteme

Eine der Besonderheiten von Smart Devices ist, dass diese in der Regel nicht mehr auf klassischen Betriebssystemen wie beispielsweise Windows, macOS oder Linux basieren, sondern auf speziellen Betriebssystemen um der neuartigen Interaktion gerecht zu werden. Verbreitete Betriebssysteme für mobile Geräte sind:

- Android (Google)
- iOS (Apple)
- Bada/Tizen (Samsung)
- WindowsPhone (Microsoft)
- Blackberry OS (RIM)
- Symbian OS (Nokia)

Mit einem Marktanteil von fast 98% (Stand März 2019)[9], beherrschen Android (75,39%) und iOS (22,35%) den Markt, weshalb sich die weitere Betrachtung auf diese beiden großen Betriebssysteme beschränkt, die sich relativ stark voneinander unterscheiden.
Android basiert auf einer Open-Source Architektur und steht im Kern zur Integration und Anpassung für Hersteller zur Individualisierung zur Verfügung: „This was, and still is in direct contrast to Apple's iOS platform which is zealously controlled by Apple Inc.“[45, P.206] iOS wurde von Apple nur für die eigene Hardware entwickelt und existiert auch nur innerhalb einer Versionshistorie.
Android-basierte Geräte lassen sich nicht nur durch den Hardwarehersteller anpassen, sondern auch durch Erweiterungen aus dem offiziellen Google PlayStore als auch freier Stores zur Verbreitung von Software. Dies ist bei iOS auch mit Zustimmung des Nutzers nicht zu erreichen. Es wird nur Software aus dem eigenen App-Store erlaubt und die dort angebotenen Apps wurden allesamt von Apple auf Funktion und Sicherheit getestet[10]. So wird beispielsweise die Identität des Entwicklers durch Apple überprüft bevor dieser Apps einreichen kann [vgl. 1, S.25]. Dieses geschlossene System lässt sich nur durch die Nutzung eines sogenannten *Jailbreaks*, einer Modifikation

[9] `http://gs.statcounter.com/os-market-share/mobile/worldwide`
[10] `https://www.apple.com/de/business/resources/docs/iOS_Security_Overview.pdf`

des Betriebssystems umgehen. Solch eine Öffnung des Betriebssystems existiert auch für Android; dort wird es als *Rooting* bezeichnet. Der Einsatz modifizierter Geräte sollte im Informationsverbund einer Institution unbedingt verhindert werden.
Hinsichtlich der Anwendungsarchitektur ähneln sich die beiden Betriebssysteme: Apps laufen in einer Sandbox[11] und haben einen exklusiv zugeordneten Speicherplatz für Programmdaten [vgl. 1, S.26]. Zugriff auf die Daten anderer Programme ist nicht möglich. Bei iOS ist außerdem auch kein echtes Multitasking realisierbar: „Apps can only perform background processing through system-provided APIs“.[1, S.26] Routinen, die die Datenströme im Hintergrund überwachen (z.B. Antivirus), sind deshalb nicht umsetzbar.
Regelmäßige Sicherheitsupdates vom Hersteller und die bereits erwähnte restriktive App-Politik geben Enterprise-Kunden ein Gefühl erhöhter Sicherheit. Android hing diesbezüglich lange Zeit zurück. Da die Hardware-Hersteller, die für ihre Geräte auf Android setzten, in diesem wichtigen Markt auch Anteile haben wollten, gibt es beispielsweise von Samsung (Knox) und LG (Gate) Konzepte um Android sicherer zu machen. Diese Konzepte der Hardware-Hersteller verbessern zwar tatsächlich die Sicherheit des Betriebssystems, können aber das fehlende Vertrauen der Enterprise-Kunden in eine nachhaltige Sicherheitsstrategie nicht vollends beseitigen. Google hat seinerseits *Android Enterprise* (vormals AndroidWork) entwickelt und kann aufgrund der tiefergreifenden Zugriffsmöglichkeiten auf den Android-Kernel einen größeren Funktionsumfang anbieten. Unterschiedliche Entwicklungsgeschwindigkeiten führen hierbei zu verschiedenen Softwareversionen. Eine Folge in diesem Zusammenhang ist, dass die im Umlauf befindlichen iOS-basierten Geräte in der Breite aktuellere Betriebssystem-Versionen einsetzen als Android-basierte Geräte. So läuft Stand März 2019 auf knapp drei Vierteln (74,74%) der im Umlauf befindlichen Geräte die aktuelle Hauptversion iOS12.[12] Bei Android laufen nur auf 37,16% der im Umlauf befindlichen Geräte Android 8, auf 11,69% Android 7, auf 16,38% noch Android 6 und gar noch auf 10,37% Android 5.[13] Dies belegt, dass iOS-Geräte eine zuverlässigere Update-Politik erfahren und Android diesbezüglich noch nicht gleichziehen konnte.

4.4 Gerätemanagement

Zum Management der Geräte durch die IT der Institution bedarf es ab einem bestimmten Funktionsumfang bzw. Skalierung einer zusätzlichen Lösung. Dienste wie

[11] Zustand, dass ein Programm in einer vom restlichen System abgeschotteten Umgebung betrieben wird.
[12] `http://gs.statcounter.com/os-version-market-share/ios/mobile-tablet/worldwide`
[13] `http://gs.statcounter.com/os-version-market-share/android/mobile-tablet/worldwide`

PIM-Funktionen und Remotedesktop-Verbindungen sind in gewissem Maße auch ohne zusätzliches Management realisierbar, aber sobald die Möglichkeit besteht, Daten auch lokal zu speichern, führt allein schon aus datenschutzrechtlichen Gründen kein Weg mehr an einem Management-Tool vorbei. Auch der Verwaltungsaufwand zum Einrichten der Geräte kann durch Einsatz einer solchen Lösung deutlich reduziert werden, da der Mitarbeiter die Registrierung in der Regel selber initiieren und die weitere Einrichtung zu großen Teilen automatisiert ablaufen kann.
Wie in Kapitel 2.3.6 bereits erwähnt, existieren, je nach Funktionsumfang, unterschiedliche Bezeichnungen für Management Lösungen. Diese unterscheiden sich wie folgt und bauen, wie in Abbildung 4.1 dargestellt, entsprechend aufeinander auf.

- **MDM** (Mobile Device Management): Bietet Funktionen zur Verwaltung eines Gerätes wie Aktualisierung des Betriebssystems, Einrichten des Nutzerkontos und Sperren sowie im drastischsten Fall Löschen aus der Ferne [19].
- **MAM** (Mobile Application Management): Hiermit lassen sich Anwendungen auf dem Gerät des Anwenders administrieren. Dabei können Verantwortliche einen eigenen AppStore einrichten oder ausschließlich bestimmte Programme aus beispielsweise Androids Play Store zulassen. Das einst favorisierte App Wrapping[14] ist bei den meisten Anbietern inzwischen jedoch nicht mehr enthalten [19]. Container-Lösungen gehören auch in diese Kategorie.
- **EMM** (Enterprise Mobility Management): Kombiniert die Funktionalitäten eines MDM mit denen eines MAM in einer Lösung.
- **CMT** (Client Management Tools): Lösungen zur Verwaltung von klassischen Clients.
- **UEM** (Unified Endpoint Management): Führt das klassische Client Management (CMT) und das Enterprise Mobility Management (EMM) in eine einheitliche Verwaltungslösung zusammen.

Das US-amerikanische Forschungsunternehmen Gartner begleitet die Entwicklung der Management-Lösungen bereits länger und veröffentlichte mittels seines *Magic Quadrant*[15] einen Überblick [vgl. 15] zu MDM (2011), EMM (2014) und UEM (2018)(siehe auch Anhang A.1).

Gartner's Ausschnitt aus dem Markt verdeutlicht, dass es eine Reihe von Anbietern zu der Management-Thematik gibt. Die Systeme sind vorwiegend Cloud-basiert (*Software-as-a-Service*) ausgeführt, teilweise aber auch noch alternativ zur Installation auf einem eigenen Server (*On-Premise*) verfügbar. Die grundlegenden MDM-Funktionen erfüllen alle genannten Lösungen. Unterschiede finden sich zumeist im

[14] Anwendung von Richtlinien (Policies) auf Apps um deren Funktionen einzuschränken.
[15] Datenanalysemethode um Markttrends aufzuzeigen.

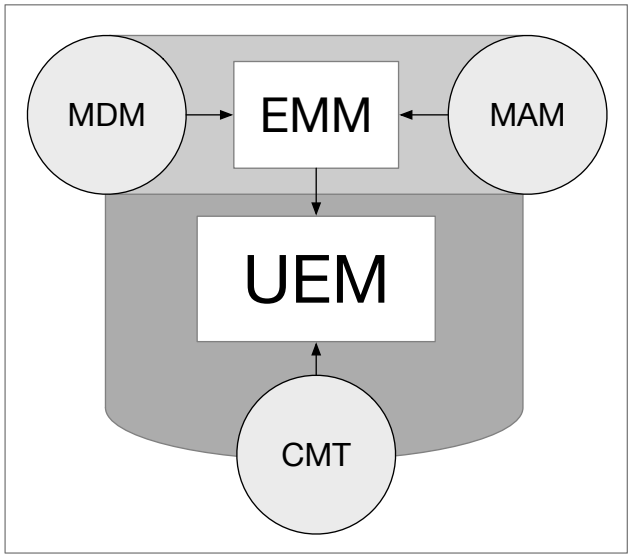

Abbildung 4.1: Zusammenhänge zwischen Management-Systemen

Ausstattungsumfang hinsichtlich erweiterter Funktionalitäten (MAM, EMM oder UEM). Bei genauer Betrachtung der Angebote muss man aber feststellen, dass die Grenzen zwischen den einzelnen Definitionen in der Praxis etwas verschwimmen und sich die Lösungen nicht immer genau in eine Kategorie einordnen lassen. Gartner nennt in seinem *Magic Quadrant* zu UEM die Lösungen von VMware, Microsoft, IBM, Blackberry und MobileIron als „Leaders“ in diesem Markt [vgl. 15].

5 Konzeption eines IT-Grundschutz Bausteins

Zur Konzeption eines neuen Bausteins für das IT-Grundschutz-Kompendium hat das BSI entsprechende Umsetzungshinweise (Version 15 vom 04.09.2017) veröffentlicht. Anhand dieser Vorgehensweise wird im Folgenden der Baustein konzipiert.

5.1 Definition des Betrachtungsgegenstandes

Zu Beginn der Untersuchung erfolgt eine Abgrenzung welche Bereiche der Institution im Baustein inkludiert werden sollen und welche nicht.

5.1.1 Schwerpunkt

Ein Baustein für BYOD muss grundsätzlich all die Vorgänge umfassen, bei denen *Geräte zugleich für private und berufliche Zwecke außerhalb des Informationsverbundes der Institution* betrieben werden. Die Konstellationen können hier sehr umfangreich sein, so dass einige Details bereits in vorhandenen Bausteinen abgebildet werden. In den Ebenen nach der Einordnung in Kapitel 2.3 könnten folgende Fragen gestellt werden:

Organisatorische Ebene

- Welche Mitarbeiter sollen die Möglichkeit für BYOD haben?
- Wie erfolgt die Anschaffung bzw. Integration der Geräte?
- In welcher Weise sind besondere Schulungsmaßnahmen erforderlich?
- Wie muss im Falle eines Verlusts bzw. Diebstahls gehandelt werden?
- Wie lassen sich Geräte wieder aus dem Programm entfernen?
- Wer verwaltet die Geräte?

- Wie sind die Besitzverhältnisse?
- Wie sind die Haftungsverantwortlichkeiten?
- Müssen zusätzliche Regelungen für den Datenschutz geschaffen werden?
- Wann dürfen Administratoren auf die Geräte zugreifen?
- ...

Applikationsebene

- Welche Software muss vorhanden sein bzw. darf nicht installiert werden?
- Welche Management-Lösung soll eingesetzt werden?
- ...

Geräteebene

- Welche Gerätekategorien, -typen oder -marken sollen unterstützt werden?
- Welche Geräteeinstellungen müssen gesetzt werden?
- ...

Diese Auflistung verdeutlicht, dass einige Fragen auf allen Ebenen anfallen können. Vor allem im organisatorischen Bereich gilt es vorab viele Aspekte hinsichtlich der Strategie zu bewerten, die die Rahmenbedingungen für die Applikations- und Geräteebene setzen. Teilweise werden die aufgeführten Fragen bereits in anderen Bausteinen behandelt. Deshalb ist es sinnvoll zunächst zu untersuchen, welche **Aspekte aus dem IT-Grundschutz in Beziehung** zu BYOD stehen:

- **ORP.2 Personal**[1]:
  Personalprobleme und menschliche Fehlhandlungen sind Gegenstand dieses Bausteins.
  Für BYOD sind die Aspekte des Ausfalls von, in diesem Zusammenhang benötigten, Administratoren und die Gefahren, die aufgrund von Sorglosigkeit und Manipulation der Mitarbeiter entstehen, nützlich.
  Input für BYOD: Vertretungsregelungen und Schulungen für Mitarbeiter.

[1] `https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_2_Personal.html`

- **ORP.3 Sensibilisierung und Schulung**[2]:
  Schärfung der Wahrnehmung der Mitarbeiter zu sicherheitsrelevanten Vorgängen und deren Behandlung durch Hinweise und Schulungen.
  Input für BYOD: Awareness für Mitarbeiter.

- **ORP.4 Identitäts- und Berechtigungsmanagement**[3]:
  Regelungen ob und falls ja in welcher Weise Mitarbeiter Zugriff auf Informationen oder Dienste der Institution haben.
  Input für BYOD: Elektronische Zugangs- und Zugriffsrechte sind bei BYOD die einzigen verfügbaren Kontrollinstrumente und deshalb von besonderer Wichtigkeit.

- **ORP.5 Compliance Management**[4]:
  Regelung des Umgangs mit vertraulichen Informationen der Institution.
  Input für BYOD: Basishinweise für sicheren IT-Betrieb.

- **CON.7 Informationssicherheit auf Auslandsreisen**[5]:
  Hinweise zur sicheren Verarbeitung von Informationen in öffentlichen Umgebungen (im In- und Ausland). **Input für BYOD: Vorsichtsmaßnahmen zum IT-Betrieb außerhalb der Institution.**

- **OPS.1.2.4 Telearbeit**[6]:
  IT-Tätigkeit, die ausschließlich außerhalb der Geschäftsräume und Gebäude des Arbeitgebers verrichtet wird (auch bei Kunden oder Lieferanten). Ziel des Schutzes der Informationen, die während der Telearbeit gespeichert, verarbeitet und übertragen werden.
  Input für BYOD: Einbindung eines von Extern agierenden Mitarbeiters in die Arbeitsabläufe der Institution sowie Hinweise zur Datensicherheit und Sensibilisierung/Schulung zu möglichen Gefährdungen. Die bei BYOD (im Falle von Consumerisation) legitimierte, private Nutzung wird unter *2.3 Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners* in diesem Szenario als kritisch eingestuft.

[2] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html
[3] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identitäts-_und_Berechtigungsmanagement.html
[4] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_5_Compliance_Management_(Anforderungsmanagement).html
[5] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_7_Informationssicherheit_auf_Auslandsreisen.html
[6] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_2_4_Telearbeit.html

- **OPS.2.4 Fernwartung**[7]:
  Informationsschutz bei aktiver und passiver Fernwartung.
  Input für BYOD: Regelungen für Fernwartung, die als Basis auch für BYOD gelten.

- **OPS.2.1 Outsourcing für Kunden**[8]:
  Bewahren der Sicherheitsziele der Institution bei der vollständigen oder teilweisen Auslagerung von Geschäftsprozessen und Dienstleistungen an einen externen Dienstleister.
  Input für BYOD: Auswahl und Kooperation mit einem Dienstleister beispielsweise bei Nutzung einer Cloud.

- **NET.2.2 WLAN-Nutzung**[9]:
  Hinweise zur sicheren Nutzung von WLANs.
  Input für BYOD: Sensibilisierung hinsichtlich Abhören und Nutzung unsicherer WLANs (Hotspots).

- **NET.3.3 VPN**[10]:
  Protokoll zur Absicherung von schutzbedürftigen Daten (Integrität und Vertraulichkeit) bei der Übertragung über nicht-vertrauenswürdige Netze. Definition von Anforderungen zur Planung, Umsetzung und Betriebs eines VPN.
  Input für BYOD: Herstellung einer sicheren Kommunikation über ein öffentliches Netzwerk. Zentrale Technologie für BYOD.

- **SYS.2.1 Allgemeiner Client**[11]:
  Allgemeine Hinweise zum Schutz von auf Clients gespeicherten Informationen unabhängig vom installierten Betriebssystem.
  Input für BYOD: Basis für den Betrieb eines Clients.

- **SYS.3.1 Laptops**[12]:
  Spezifische Hinweise zum sicheren Betrieb eines Laptops.
  Input für BYOD: Fokussierung auf zusätzliche Gefahren mobiler IT-Nutzung.

[7] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_2_4_Fernwartung.html
[8] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_2_1_Outsourcing_für_Kunden.html
[9] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_2_2_WLAN-Nutzung.html
[10] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_3_VPN.html
[11] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_2_1_Allgemeiner_Client.html
[12] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_1_Laptops.html

- **SYS.2.2.2 Clients unter Windows 8.1, SYS.2.2.3 Clients unter Windows 10, SYS.2.3 Clients unter Unix und SYS.2.4 Clients unter macOS**:
  Betriebssystemspezifische Hinweise zu Schadprogrammen, Schwachstellen und Cloud-Integration.

- **SYS.3.2.1 Allgemeine Smartphones und Tablets**[13]:
  Aufzeigen von typischen Gefährdungen für Smartphones und Tablets ohne weitere Spezifizierung ob es sich um dienstliche oder private Geräte handelt.
  Input für BYOD: Es werden bereits zwei konkrete Gefährdungen zu BYOD angesprochen: *2 9 Gefahren durch private Nutzung mobiler Geräte* und *2 10 Gefahren durch Bring Your Own Device (BYOD).*

- **SYS.3.2.3 iOS[14] und SYS.3.2.4 Android[15]**:
  Betriebssystemspezifische Hinweise zu Besonderheiten der beiden verbreiteten mobilen Betriebssysteme.
  Input für BYOD: Allgemein gültige Gefährdungen, die auch für BYOD zutreffen.

- **SYS.3.2.2 Mobile Device Management (MDM)**[16]:
  Hinweise zum sicheren Aufbau und Betrieb eines MDM zur Verwaltung und Überwachung eines Geräts aus der Ferne.
  Input für BYOD: Als eine Möglichkeit der Geräteverwaltung eine zentrale Ressource für BYOD.

- **INF.8 Häuslicher Arbeitsplatz**[17]:
  Schutz der Daten der Institution am häuslichen Arbeitsplatz (ortsfest mit Zugang durch Dritte). Keine Berücksichtigung von Sicherheitsanforderungen an die eingesetzten IT-Systeme.
  Für BYOD wird hier ein sehr verbreitetes Anwendungsszenario (Organisatorische Regelungen für den häuslichen Arbeitsplatz z.B. bei Homeoffice) behandelt. Mobiles Arbeiten und vor allem kombinierte berufliche und private Nutzung werden nicht betrachtet.
  Input für BYOD: Regelungen zum geeigneten häuslichen Arbeitsplatz und zum Umgang mit betrieblichen Informationen.

[13] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_2_1_Allgemeine_Smartphones_und_Tablets.html
[14] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_2_3_iOS_(for_Enterprise).html
[15] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_2_4_Android.html
[16] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_2_2_Mobile_Device_Management_(MDM).html
[17] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_8_Häuslicher_Arbeitsplatz.html

- **INF.9 Mobiler Arbeitsplatz**[18]:
  Thematisiert wechselnde, mobile Arbeitsplätze in unterschiedlichen Umgebungen und die damit einhergehende Notwendigkeit zum angemessenen Schutz der verarbeiteten Daten. Berücksichtigt wird ebenfalls die Problematik, dass in mobilen Arbeitsplatz-Umgebungen keine sichere IT-Infrastruktur, wie sie in einer Büroumgebung anzutreffen ist, vorausgesetzt werden kann. Formulierung von Sicherheitsanforderungen um für mobile Arbeitsplätze eine, einem Büroraum vergleichbare Sicherheitssituation zu schaffen.
  Input für BYOD: Organisatorische Regelungen zum ortsunabhängigen Arbeiten. Keine technischen Aspekte und keine Berücksichtigung gemischter Besitzverhältnisse.

Das Schaubild aus Abb.5.1 zeigt die Bausteine, die Aspekte für BYOD enthalten.

Es zeigt sich, dass der Zusatz **„zugleich für private und berufliche Zwecke“** in diesem Zusammenhang besonders prägend für BYOD ist. Genau diese kombinierte Nutzung ist eine Besonderheit, die bisher noch nicht explizit im IT-Grundschutz vertreten ist.

Eine weiterer besonderer Aspekt ist bei den Besitzverhältnissen ausfindig zu machen. Bei BYOD gehört die eingesetzte Hardware ggf. teilweise oder gar vollständig dem Mitarbeiter. Ein **Arbeitsmittel, dass nicht vollständig im Besitz der Institution ist**, ist ebenfalls noch nicht adäquat im IT-Grundschutz vertreten.

Zusätzlich lässt sich noch die **verstärkte Verantwortung des Mitarbeiters** feststellen. Viele sicherheitstechnische Aspekte, die sonst (auch mittels IT-Grundschutz) durch die Institution geregelt werden, sind außerhalb im Verantwortungsbereich des Mitarbeiters. Deshalb ist bei BYOD auch eine entsprechende Eigeninitiative des Mitarbeiters von Nöten.

Zusammenfassend lässt sich für den **Schwerpunkt des Bausteins** festhalten, dass sich dieser auf die **Betrachtung von zugleich beruflich und privat genutzten mobilen Endgeräten bezieht, die sich teilweise oder vollständig im Besitz des Mitarbeiters befinden**.

5.1.2 Sicherheitsziele

Bezüglich der Sicherheitsziele sind folgende Aspekte mit in Betracht zu ziehen:

[18] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_9_Mobiler_Arbeitsplatz.html

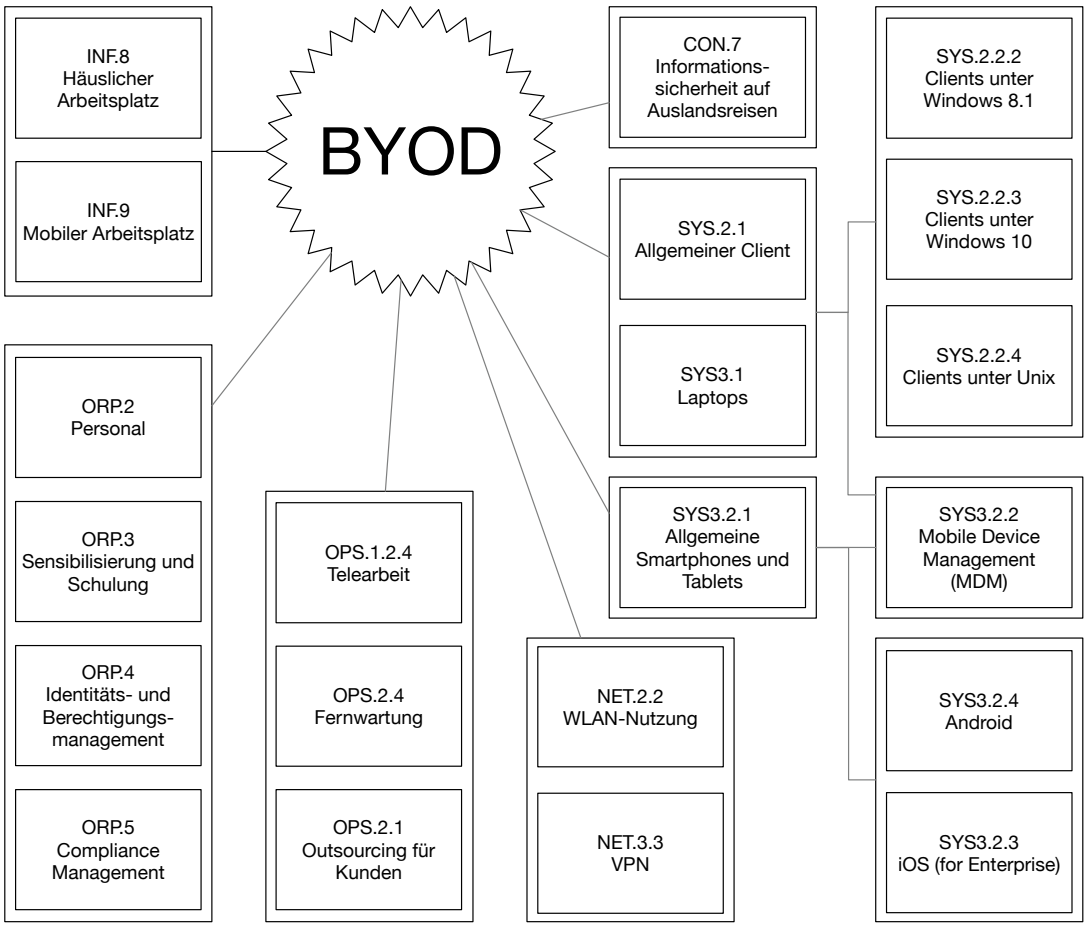

Abbildung 5.1: Bausteine aus dem IT-Grundschutz-Kompendium mit Bezug zu BYOD

- Welche Informationen können im Rahmen von BYOD ausgetauscht werden und welchen Stellenwert haben diese für die Institution?
- Welche per BYOD angebotenen Dienste bieten einen Mehrwert für die Institution?
- Würde der Ausfall eines per BYOD aktiven Mitarbeiters andere Arbeitsabläufe kritisch beeinflussen?

Anhand dieser Fragen kann der Stellenwert und die Qualität von BYOD für die Institution festgemacht werden. Falls BYOD als kritischer Prozess (hohe Priorität) eingeordnet werden kann, so müssen die Sicherheitsziele höher angesetzt werden, als wenn es sich lediglich um nebenläufige Prozesse handelt.

Im Falle der in Kapitel 2.4 vorgestellten Unternehmen wurden mittels BYOD primär PIM-Aufgaben ermöglicht und ein Remotezugang auf einen virtuellen Client realisiert.

Auch erweiterte Möglichkeiten werden als optional eingestuft. Es besteht also in der Regel immer noch ein primäres Arbeitsmittel zur Erledigung der Aufgaben. Dieses verbreitet anzutreffende Nutzungsprofil kann lediglich zu einer Gefährdung der Verfügbarkeit führen. Passiert es hingegen, dass ein hochrangiger Mitarbeiter zufällig im Ausland verweilt, während er zeitgleich wichtige Daten für einen Rollout[19] eingeben muss, so kann sich BYOD schon zum kritischen Faktor entwickeln und es müssten höhere Sicherheitsziele angesetzt werden.

Ein weiterer Faktor ist das Branchenumfeld, in dem sich die Institution bewegt. Der damit verbundene Risikoappetit[20] hängt von einer Vielzahl von Faktoren ab und bestimmt die Risikoneigung der Institution [vgl. 11, S.42]. Beispielsweise sollten Institutionen aus dem Finanzsektor mit Risiken konservativer umgehen als Unternehmen anderer Branchen.

Für die durchschnittliche Nutzung von BYOD können folgende Sicherheitsziele empfohlen werden:

- Jegliche Kommunikation muss **verschlüsselt** erfolgen.
- Es müssen **sichere Kennwörter** verwendet werden, die **regelmäßig geändert** werden müssen. Diese sollten nicht an anderer Stelle eingesetzt werden.
- Jeder Mitarbeiter, der BYOD einsetzt, muss über entsprechende Kenntnisse von **Vorsichts- und Notfallmaßnahmen** verfügen.
- Es dürfen nur **freigegebene** und entsprechend **konfigurierte Geräte** (ggf. mit Unterstützung einer Management-Lösung) eingebunden werden.

5.1.3 Zielgruppe/Anwenderkreis

Die Einsatzmöglichkeiten für BYOD sind sehr vielfältig und damit auch die potentielle Zielgruppe. Grundsätzlich ist BYOD für die Institutionen von Interesse, die im größeren Maße Informationstechnik zur Erledigung der Arbeit einsetzen. Im mittelständischen Bereich basiert der Einsatz von Informationstechnik in der Regel auf dem Arbeitsfeld und der Unternehmensgröße. Beispielsweise wird ein kleiner Handwerksbetrieb vermutlich nicht in dem Maße BYOD betreiben, wie es eine Steuerberater-Kanzlei machen könnte. Festzuhalten bleibt aber, dass die potentiellen Einsatzgebiete für BYOD unabhängig von der Branche in Zukunft eher noch zunehmen werden, so dass dieses Thema bereits heute eine große Zielgruppe im institutionalen Umfeld hat und zukünftig voraussichtlich noch steigern wird.

[19] Veröffentlichungsvorgang neuer Softwareprodukte bzw. Integration in vorhandene Infrastruktur.

[20] Durch kulturelle, interne, externe oder wirtschaftliche Einflüsse entstandene Neigung einer Institution, wie sie Risiken einschätzt, bewertet und mit ihnen umgeht.

5.1.4 Gerätekategorien

In Zeiten von IoT[21] gibt es immer mehr Geräte, die potentiell für BYOD in Frage kämen. Unrealistisch wäre es aber beispielsweise davon auszugehen, dass ein Mitarbeiter einen smarten Lautsprecher sinnvoll kombiniert zu Hause und im Institutionsnetzwerk einsetzen könnte. Die (nach heutigem Stand) für BYOD zur Auswahl stehenden Gerätekategorien sind:

- **Computer:** Als mobile Variante ist der **Laptop** bzw. das **Notebook** am häufigsten im Rahmen von BYOD anzutreffen, aber auch stationäre Desktop-Computer können im Homeoffice eingesetzt werden. Aufgrund der vielfältigen Konfigurationsmöglichkeiten sind die klassischen Computer jedoch auch die komplexeste Variante. Verbreitete Betriebssysteme dieser Gruppe sind:
  - Microsoft Windows, aktuell in Version 10, Marktanteil 09/2018: 81,76%[22]
  - Apple macOS, aktuell in Version 10.14, Marktanteil 09/2018: 13,49%[22]
  - Linux in diversen Distributionen, Marktanteil 09/2018: 1,68%[22]
- **Smartphone:** Mit immer leistungsfähigeren Geräten sind heute einige Praxisanwendungen realisierbar, die früher nur auf großen Rechnern möglich waren. Eine Vielzahl von verfügbaren Apps bieten zugleich Chancen und Risiken. Hinsichtlich der eingesetzten Betriebssysteme konzentriert sich der Markt aktuell auf zwei große Distributionen (vgl. Kap.4.3):
  - Google Android, Marktanteil 09/2018: 71,07%[23]
  - Apple iOS, Marktanteil 09/2018: 27,77%[23]
- **Tablet/Phablet:** Als weitere Kategorie haben auch Tablets ihren Anteil im institutionalen Umfeld. Diese per Touch-Eingabe gesteuerten Bildschirme ohne feste Tastatur können mit gestiegener Leistungsfähigkeit heute ebenfalls viele auftretende Anforderungen erfüllen. Je nach Ausstattung können mit diesen Geräten auch im Mobilfunknetz Daten ausgetauscht und telefoniert werden. Dann verschwimmen die Grenzen zwischen Smartphones und Tablets in eine weitere Kategorie, den Phablets. Die eingesetzten Betriebssysteme entsprechen den Varianten auf den Smartphones (mit optischen Anpassungen aufgrund der vergrößerten Darstellungsfläche).

[21] Internet-of-Things steht für die Vernetzung von Alltagsgegenständen, die (teilweise mittels proprietärer Betriebssysteme) miteinander kommunizieren können.

[22] `https://de.statista.com/statistik/daten/studie/157902/umfrage/marktanteil-der-genutzten-betriebssysteme-weltweit-seit-2009/`

[23] `https://de.statista.com/statistik/daten/studie/184332/umfrage/marktanteil-der-mobilen-betriebssysteme-in-deutschland-seit-2009/`

- **Wearables:** Mit Blick voraus sind noch die Wearables zu erwähnen, die voraussichtlich zukünftig einige Funktionen der Smartphones miniaturisieren werden. Etwas weiter in der Zukunft könnten auch smarte Brillen Einzug in den Alltag halten. In diesem Zusammenhang wird bereits von *WYOD (Wear Your Own Device)* gesprochen.

5.1.5 Zielobjekte

Wie in Kapitel 5.1.1 gezeigt, ist BYOD grundsätzlich ein Konzept für die zugleich private und berufliche Nutzung eines, im Eigentum des Arbeitnehmers befindlichen, mobilen Endgeräts. Der Umfang dieser Nutzung und die damit verbundenen eingesetzten Ressourcen sind im hohen Maße flexibel. Während kleinere Betriebe beispielsweise lediglich einen Cloud-Dienst zum Datei-Austausch mit ihren Mitarbeitern nutzen könnten, so könnten größere Institutionen beispielsweise Remote-Virtualisierungen auf, mittels VPN verbundenen, eigenen Servern betreiben. Je nach Ausprägung der Nutzung hilft es dafür unterschiedliche Zielobjekte verschiedener Gattungen zu betrachten und in die Planungen mit einzubeziehen:

- **Lokale Endgeräte (LD):** Zu dieser Gruppe zählt in diesem Kontext der stationäre Desktop-Computer, der von zu Hause beruflich im Rahmen von Homeoffice eingesetzt wird.
- **Mobile Endgeräte (MD):** Als mobile Endgeräte kommen in der Praxis aktuell Laptops, Smartphones oder Tablets zum Einsatz. Durch die zunehmende Leistungsfähigkeit der Smartphones und Tablets, können diese hinsichtlich der Zielobjekte, zusammen mit den Laptops, als eine Gruppe geführt werden. Zukünftig könnte auch die Gruppe der Wearables an Bedeutung gewinnen. Siehe auch Kap.5.1.4.
- **Lokale Nutzung (LU):** Die Benutzung eines mobilen Endgerätes kann sich durchaus auch auf die rein lokale Nutzung beschränken. In diesem Kontext werden beispielsweise nur auf dem Gerät gespeicherte Excel-Listen abgefragt. Dieses Einsatzszenario kann bei zunehmender Nutzung schnell zu Synchronisationsproblemen führen, da ein Abgleich regelmäßig manuell angestossen werden müsste.
- **Online Nutzung (OU):** Die meisten mobilen Endgeräte bieten von Hause aus eine Verbindung ins Internet. Auch Laptops werden heute teilweise mit einer eingebauten Mobilfunk-Option angeboten. Zusätzlich sind an immer mehr Standorten auch (öffentliche) W-Lan-Netzwerke verfügbar. Damit lassen sich Internetdienste wie beispielsweise Mail- oder Cloud-Services nutzen. Diese können entweder über den Unternehmensserver (CS) angeboten oder durch einen externen Dienstleistungsserver (PS) bereitgestellt werden.

- **Remote Nutzung (RU):** Bei der Remote-Nutzung wird die Kommunikationsverbindung nur dazu genutzt, ein Videosignal samt Steuerbefehlen zu transferieren. Der eigentliche Arbeitsprozess findet in einer virtuellen Session auf einem entfernten Server statt. In der Regel handelt es sich bei diesen Servern um eigene Unternehmensserver. Aber auch für Virtualisierungen gibt es heute Angebote von externen Dienstleistern.
- **Kommunikationsverbindung (CC):** Je nach Anwendungsfall läuft die Verbindung über unterschiedliche Wege (WLAN, LTE, 3G oder Edge) und verschiedene Protokolle. In diesem Zusammenhang sehr verbreitet ist beispielsweise das VPN-Protokoll (Kap.2.3.3) als Grundlage einer sicheren Kommunikation über öffentliche Netze.
- **Dienstleistungsserver (PS):** Bestimmte Aufgaben, wie beispielsweise Cloud-Dienste oder Exchange-Services, können auch bei einem externen Dienstleister gehostet werden. Die Institution fungiert in diesem Fall als Auftraggeber und der Server steht nicht im Verantwortungsbereich. Dies wird oftmals dann eingesetzt, wenn es sich um eine kleinere Institution handelt oder die Institution das Risiko eines eigenen Betriebs scheut (Risikotransfer).
- **Unternehmensserver (CS):** Ein von der Institution selber betriebener Server kann beispielsweise als Dateiserver fungieren oder auch Virtualisierung anbieten. Dieser Server steht im Verantwortungsbereich der Institution.
- **Administrationsserver (AS):** Dieser Server dient dazu, das mobile Endgerät aus der Ferne zu administrieren. Er kann sowohl extern (Dienstleister) wie auch intern (Institut) betrieben werden. Es können einfache Funktionen wie beispielsweise eine GPS-Ortung oder eine Remote-Sperrung oder umfangreichere Dienste (mittels MDM-Software) eingesetzt werden.

Das Schaubild aus Abb.5.2 stellt diese Zielobjekte in Beziehung.

5.2 Recherche

Basierend auf der allgemeinen Recherche zum Thema in den Kapiteln 2, 3 und 4, fließen die Ergebnisse in die Konzeption des Bausteins mit ein.

5.3 Ermittlung von Gefährdungen

Den Vorgehenshinweisen des BSI folgend werden zur Ermittlung von Gefährdungen zunächst die elementaren Gefährdungen hinsichtlich des Betrachtungsgegenstandes

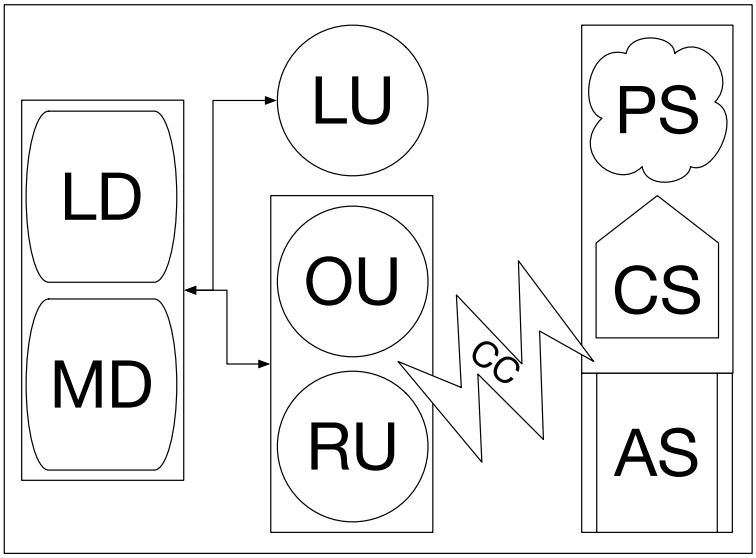

Abbildung 5.2: Zielobjekte des Betrachtungsgegenstandes zu BYOD

bewertet.

5.3.1 Bewertung elementarer Gefährdungen

- **G 0.01 Feuer:** Diese elementare Gefährdung könnte einzelne BYOD-Geräte oder damit im Zusammenhang stehende Kommunikationsserver gefährden. Da der Funktionsausfall von BYOD aber nur eine Folge davon wäre, ist hier von einer **indirekten** Gefährdung zu sprechen. Da sich die Standorte des BYOD-Benutzers in der Regel ändern, würde sich diese Gefährdung auf dieser Seite standardisiert nur schwierig handhaben lassen.
- **G 0.02 Ungünstige klimatische Bedingungen:** Diese potentielle Gefährdung bezieht sich auf die Umgebung, in der die im Rahmen von BYOD genutzten Geräte betrieben werden. Kälte kann beispielsweise ein größeres Problem für Akkus in mobilen Geräten darstellen. Weisen diese eine Schwäche auf, so kann durch Kälteeinflüsse im schlimmsten Fall eine sofortige Abschaltung des Gerätes eintreten. Ebenso kann Hitze oder übermäßige Luftfeuchtigkeit elektronischen Geräten Schäden zuführen. Auch in diesem Fall sind BYOD-Teilnehmer von Ausfällen durch eine **indirekte** Gefährdung bedroht.
- **G 0.03 Wasser:** Die Steigerung von Feuchtigkeit in Form von Regen oder Spritzwasser ist Wasser ggf. mit entsprechendem Druck. Dieses kann auch einzelne BYOD-Komponenten gefährden und ist als **indirekte** Gefahr einzustufen. Mittlerweile gibt es beispielsweise bereits Geräte, die eine Wasserdichtigkeit

nach dem IP-Standard[24]. Ist vorhersehbar, dass ein, im Rahmen von BYOD genutztes Gerät, in nassen Bedingungen zum Einsatz kommen soll, so sollte auf die entsprechende Schutzklasse geachtet werden.

- **G 0.04 Verschmutzung, Staub, Korrosion:** Unvorsichtiger Umgang mit empfindlichen Geräten oder Datenträgern, die im Rahmen von BYOD eingesetzt werden, kann zu schädlichem Einfluss von Schmutz oder Feuchtigkeit führen und die Verfügbarkeit oder Integrität beeinträchtigen. Neben robusteren Geräten/Datenträgern (z.B. IP-Standard[24]), kann entsprechende Sensibilisierung der Nutzer die Gefahr mindern. Auch diese Gefährdung ist als **indirekt** einzuordnen.
- **G 0.05 Naturkatastrophen:** Durch seismische, klimatische oder vulkanische Phänomene ausgelöste Naturkatastrophen können auch die an der BYOD-Kommunikation beteiligten Komponenten negativ beeinflussen. Hauptsächlich könnte dies Versorgungsleitungen betreffen und eine **indirekte** Bedrohung für BYOD darstellen.
- **G 0.06 Katastrophen im Umfeld:** Bedrohliche Ereignisse in unmittelbarer Nähe gefährden Infrastruktur und Personen. Hinsichtlich BYOD handelt es sich um eine **indirekte** Gefährdung.
- **G 0.07 Großereignisse im Umfeld:** Veranstaltungen oder Unruhen im Umfeld können die Infrastruktur und Personen gefährden und für BYOD eine **indirekte** Gefährdung darstellen.
- **G 0.08 Ausfall oder Störung der Stromversorgung:** Da mobile Geräte, wie sie oftmals bei BYOD genutzt werden, in der Regel über einen Akku verfügen, sind diese gegen einen vorübergehenden Stromausfall gewappnet. Anders sieht das bei der Kommunikations-Infrastruktur und dem Institutions-Netz aus. Hier kann ein Stromausfall (sofern diese nicht mittels einer so genannten USV[25] abgesichert sind) die Verfügbarkeit und die Integrität gefährden, weshalb diese Gefährdung als **indirekt** eingestuft werden kann.
- **G 0.09 Ausfall oder Störung von Kommunikationsnetzen:** Fallen Kommunikationsverbindungen über eine längere Zeit aus, so stellt dies eine **indirekte** Gefährdung für BYOD dar, da viele Prozesse eine funktionierende Kommunikationsverbindung benötigen. Redundanz (z.B. WLan und alternativ Mobilfunk) kann das Risiko mindern.

[24] Eignung von elektrischen Betriebsmitteln für verschiedene Umgebungsbedingungen. Die beiden nachfolgenden Ziffern kennzeichnen die genaue Widerstandsfähigkeit, wobei die erste Ziffer den Schutz gegen Fremdkörper/Berührung und die zweite Ziffer den Schutz gegen Wasser klassifiziert. Beispielsweise bedeutet IP54: Geschützt gegen Staub in schädigender Menge und gegen allseitiges Spritzwasser.

[25] Unterbrechungsfreie Stromversorgung

- **G 0.10 Ausfall oder Störung von Versorgungsnetzen:** Schäden in Versorgungsnetzen können Einfluss auf Server oder Kommunikations-Infrastruktur haben und damit eine **indirekte** Bedrohung für BYOD darstellen.
- **G 0.11 Ausfall oder Störung von Dienstleistern:** Aufgrund der Notwendigkeit einer intakten Kommunikationsstruktur, würde ein Ausfall des Kommunikationsdienstleisters zum partiellen oder gar vollständigen Ausfall des Systems führen. Dieser **indirekten** Bedrohung kann durch entsprechende Auswahl der Dienstleister (Zertifizierung) und redundanter Lösungen (alternatives Kommunikationsnetz) begegnet werden.
- **G 0.12 Elektromagnetische Störstrahlung:** Da die Endgeräte bei BYOD teilweise auch auf eine funktionierende Kommunikationsverbindung angewiesen sind, ist eine Beeinflussung durch elektromagnetische Störstrahlung eine **indirekte** Gefährdung.
- **G 0.13 Abfangen kompromittierender Strahlung:** Mobile Geräte können über verschiedene Funkschnittstellen kommunizieren. Angefangen bei Funktechnologien, die nur in unmittelbarer Nähe funktionieren (*NFC* oder *Bluetooth*) über *Wireless LAN* bis hin zu *3G* bzw. *LTE*. Je nach gewählter Schnittstelle besteht die Gefahr, dass die Kommunikation abgefangen werden kann. Dies ist zwar nicht spezifisch für BYOD aber doch aufgrund der Vielzahl von Schnittstellen und den äußeren Einflüssen im öffentlichen Raum verstärkt gültig. Die Einordnung erfolgt deshalb als **indirekte** Gefährdung. Die gängigen Protokolle für diese Kommunikationsvarianten bieten durch den Einsatz geeigneter Verschlüsselungsverfahren bereits einen Schutz gegenüber unberechtigtem Abhören.
- **G 0.14 Ausspähen von Informationen/Spionage:** Abseits technischer Möglichkeiten zum Abfangen der Kommunikation, existieren auch andere Faktoren, die dazu führen können, dass beim Einsatz von BYOD Daten an Unbefugte gelangen und das Konzept damit einer **direkten** Gefährdung ausgesetzt ist. Triviale Ursachen wie Abschauen von Informationen bei der Nutzung im öffentlichen Raum sind zumeist auf leichtsinniges Verhalten der Anwender zurückzuführen. Dieses Risiko ist durch Schulungsmaßnahmen und der Kenntnisnahme von Verhaltensregeln seitens der Anwender reduzierbar.
- **G 0.15 Abhören:** BYOD ist für klassisches Abhören von Informationen stärker gefährdet. Die diversen Einsatzszenarien bergen immer wieder Berührungspunkte mit Unbeteiligten. Umso mehr ist darauf zu achten, dass vertrauliche Informationen nicht laut vorgelesen oder Telefongespräche mit vertraulichen Informationen in diesen Umgebungen geführt werden. Diese **direkte** Gefährdung kann durch Verhaltensmaßnahmen der BYOD-Anwender lediglich teilweise entschärft werden. Wie es beispielsweise im Unternehmen sinnvoll sein kann

bei vertraulichen Gesprächen die Fenster und Türen geschlossen zu halten, so kann dies auch auf BYOD bezogen (beispielsweise zu Hause) ein sinnvolles Mittel sein. Im öffentlichen Raum sind diese Maßnahmen allerdings nicht immer realisierbar, weshalb hier abhörgefährdete Aktionen vermieden werden sollten.

- **G 0.16 Diebstahl von Geräten, Datenträgern und Dokumenten:** Unter Diebstahl ist in diesem Fall das bewusste Entwenden von, im Rahmen von BYOD genutzten Geräten, Daten oder Dokumenten gemeint. Grundsätzlich stellt dies eine **direkte** Bedrohung für die Institution dar und es sollte von Beginn an Wert darauf gelegt werden, den Schaden im Verlustfall so gering wie möglich zu halten. Bei Geräten und Daten in Kombination mit BYOD sollten sowohl proaktive als auch reaktive Maßnahmen eingeführt werden. Dies sind beispielsweise sichere Passwörter, regelmäßige Backups, erhöhte Sorgfalt im Umgang mit Daten und Geräten sowie Einsatz effektiver Verschlüsselungsverfahren auf der proaktiven und Mechanismen zur Remote-Sperrung oder -Löschung des Gerätes auf der reaktiven Seite.
- **G 0.17 Verlust von Geräten, Datenträgern und Dokumenten:** Verlust ist gegenüber Diebstahl ein Vorgang, bei dem nicht zwingend davon ausgegangen werden muss, dass eine bedrohliche Absicht dahintersteckt. Im Ergebnis sind die Daten/Geräte aber trotzdem verloren und müssen vor unbefugtem Zugriff geschützt werden. Hierfür sind grundsätzlich dieselben proaktiven und reaktiven Maßnahmen nötig wie bei G 0.16. Hinsichtlich BYOD ist durch den hauptsächlichen Einsatz außerhalb des Informationsverbundes das Risiko für einen Verlust erhöht und es stellt eine **direkte** Bedrohung dar.
- **G 0.18 Fehlplanung oder fehlende Anpassung:** Fehlende Vorausschau und Anpassung an neue Gegebenheiten kann ein **direktes** Risiko für BYOD bedeuten. Es können beispielsweise durch Auswahl ungeeigneter Übertragungsprotokolle Schwachstellen entstehen.
- **G 0.19 Offenlegung schützenswerter Informationen:** Ein Verlust der Vertraulichkeit von Daten und Informationen wie Passwörtern ist eine **direkte** Gefährdung für BYOD, da die Authentifizierung sehr oft nur durch diese Daten sichergestellt werden kann. Wenn man beispielsweise durch einen Passwortverlust eventuell gar nicht bemerkt, dass sich jemand einer anderen Identität bedient, so sind die damit verbundenen Prozesse nicht mehr sicher.
- **G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle:** Informationen, Software oder Geräte nicht verifizierter Herkunft sind grundsätzlich eine **direkte** Gefährdung für BYOD, da beispielsweise durch einen Eingriff modifizierte Endgeräte nicht sicher einsetzbar sind.
- **G 0.21 Manipulation von Hard- und Software:** Eingriffe in die Hardware oder beispielsweise durch Trojaner kontrollierte Software können dazu

führen, dass auch eine im Rahmen von BYOD genutzte, eigentlich sichere Kommunikationskette unterwandert werden kann. Abseits gängiger Methoden. wie dem regelmäßigen Einsatz von Antiviren- und Anti-Spyware-Software zur Verhinderung von Software-Eingriffen oder beispielsweise Verhaltensmaßnahmen zur Risiko-Minderung von Hardware-Manipulationen, ist diese **direkte** Gefährdung aufgrund der vielfältigen Ausprägungen schwer zu minimieren.

- **G 0.22 Manipulation von Informationen:** Durch gezielten Eingriff in die Kommunikationskette, die im Rahmen von BYOD den entfernten Nutzer mit dem Informationsverbund der Institution verbindet, können Informationen ggf. manipuliert werden. Diese **indirekte** Gefährdung wird durch den Einsatz sicherer Kommunikationsprotokolle mit Verschlüsselung verringert. Deshalb sollte darauf geachtet werden, dass alle eingesetzten Programme auch die entsprechend sichere Kommunikation unterstützen.
- **G 0.23 Unbefugtes Eindringen in IT-Systeme:** Wenn jemand unbefugt Zugang zu IT-Systemen erlangt, so kann er in der Regel auch Einfluss auf die Geräte nehmen. Dies wäre eine **indirekte** Bedrohung für BYOD, da eine sichere Kommunikationskette dann nicht mehr garantiert werden kann.
- **G 0.24 Zerstörung von Geräten oder Datenträgern:** Versehentliche oder mutwillige Beschädigung von Geräten oder Datenträgern ist eine **indirekte** Bedrohung für BYOD da diese dann nicht mehr nutzbar sind. Bei BYOD erhöht sich gegenüber der Nutzung innerhalb des Informationsverbundes der Institution das Risiko für Beschädigungen, da der Kontakt mit der Umwelt weitaus umfangreicher sein kann.
- **G 0.25 Ausfall von Geräten oder Systemen:** Ausfälle von für BYOD genutzten Gerätschaften können eine **indirekte** Gefährdung darstellen. Dies ist jedoch abhängig von der Nutzungsweise. So ist es beispielsweise recht einfach möglich eine Remotedesktopverbindung bei Ausfall eines Clients auf einem anderen Client zu benutzen.
- **G 0.26 Fehlfunktion von Geräten oder Systemen:** Hinsichtlich einer fehlerhaften Funktion von BYOD-genutzten Komponenten muss unterschieden werden, ob es sich hierbei um ein Funktionsversagen oder um ein schädliches Fehlverhalten handelt. Gerade im letztgenannten Fall besteht eine **direkte** Gefährdung für BYOD.
- **G 0.27 Ressourcenmangel:** Nicht ausreichend dimensionierte Datenleitungen oder Geräteressourcen stellen eine **direkte** Gefährdung für BYOD dar. Ist der Mangel nur schwach ausgeprägt, wird sich dies durch unzureichende Performance und damit fehlende Akzeptanz der Nutzer äußern. Fällt eine notwendige Ressource aber unter ein, für den Betrieb notwendiges Maß, so führt dies zu einem Ausfall.

- **G 0.28 Software-Schwachstellen oder -Fehler:** Je mehr Funktionen eine Software umfasst, desto öfters können Fehler auftreten, die auch mittels umfangreicher Tests nicht immer im Vorfeld erkannt werden können. Softwarefehler können im späteren Einsatz zu Ausfällen, aber auch zu Fehlergebnissen führen. Weiter können Softwarefehler Einfallstore für Schadsoftware darstellen. Diese Bedrohung ist nicht spezifisch für BYOD, sondern allgemein gültig und deshalb als **indirekt** einzuordnen.

- **G 0.29 Verstoß gegen Gesetze oder Regelungen:** Werden geltende Gesetze oder Regelungen missachtet, kann dies zu großen Problemen für die Institution führen. Werden beispielsweise personenbezogene Daten über eine ungesicherte Verbindung übertragen, so führt dies ggf. zu einer Verletzung des Datenschutzes. Im Rahmen von BYOD ist dies nicht anders als generell in der Institution notwendig und es kann von einer **indirekten** Bedrohung ausgegangen werden.

- **G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen:** Eine unberechtigte Nutzung kann aufgrund diverser Faktoren (Zutritt, Zugriff, Zugang) auftreten. Bei BYOD sind diese Faktoren aufgrund der Verlagerung des Einsatzbereiches primär außerhalb des Informationsverbundes und der oftmals gemischt privat und dienstlich stattfindenden Nutzung verstärkt. Es kann von einer **indirekten** Gefährdung gesprochen werden.

- **G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen:** Konfigurationsfehler können sich generell negativ auf die Zuverlässigkeit von Geräten und Systemen auswirken. Da jedoch in Kombination mit BYOD eine kombinierte private und dienstliche Nutzung desselben Gerätes vorliegt und damit einhergehend die Anforderung des Nutzers besteht, im privaten Bereich Administrationsrechte zu besitzen, sind hier erweiterte Anforderungen zu berücksichtigen. Diese Gefährdung kann als **indirekt** eingestuft werden.

- **G 0.32 Missbrauch von Berechtigungen:** Diese **indirekte** Gefährdung tritt dann ein, wenn recht- oder unrechtmäßig erworbene Berechtigungen in einer Weise genutzt werden, wie dies ursprünglich nicht vorgesehen war. Im Zusammenhang mit BYOD kann dies zum Beispiel dann auftreten, wenn der Nutzer aufgrund der kombinierten privaten und beruflichen Nutzung des Gerätes höhere Berechtigungen hat, als dies auf der beruflichen Seite notwendig wäre.

- **G 0.33 Personalausfall:** Damit BYOD richtig funktionieren kann, müssen seitens der Institution einige zusätzliche Dienste angeboten werden. Diese bedürfen ggf. der Betreuung durch spezialisierte Mitarbeiter. Ein Ausfall dieser Mitarbeiter muss seitens der Institution umgehend adäquat ersetzt werden

können. Dieser **indirekten** Gefährdung könnte mittels regelmäßiger Schulungen und Multiplikatoren sowie redundanter Stellenbesetzung begegnet werden.

- **G 0.34 Anschlag:** Ein Angriff auf Institutionseinrichtungen, kann auch für BYOD notwendige technische Komponenten betreffen. Zur Absicherung gegen diese **indirekte** Gefährdung ist vor allem ein Datenverlust zu vermeiden.
- **G 0.35 Nötigung, Erpressung oder Korruption:** Im Rahmen dieser **indirekten** Gefährdung wäre es denkbar, dass auch für BYOD notwendige Passwörter oder Verschlüsselungsdaten in falsche Hände geraten.
- **G 0.36 Identitätsdiebstahl:** Hinsichtlich BYOD stellt sich diese **direkte** Gefährdung noch etwas verstärkt dar, da aufgrund des Betriebs außerhalb der Institutionsgrenzen viele zusätzliche Schutzmaßnahmen wie beispielsweise Zugangsberechtigungen keinen Einfluss haben. Deshalb liegt der Schutz vor Identitätsdiebstahl vor allem im technischen Bereich, zum Beispiel durch die Qualität von Passwörtern (ggf. mit Zwei-Faktor-Authentifizierung), dem verwendeten Protokoll oder den eingesetzten Verschlüsselungsverfahren.
- **G 0.37 Abstreiten von Handlungen:** Die Verbindlichkeit ist in der Informationssicherheit ein wichtiger Faktor. Mittels des Einsatzes digitaler Signaturen gibt es auch technische Werkzeuge um die Nichtabstreitbarkeit (Non-Repudiation) sicherzustellen. Hinsichtlich BYOD ist die Nichtabstreitbarkeit ein wichtiges Merkmal damit das Verfahren funktionieren kann. Aus diesem Grunde ist hier von einer **direkten** Gefährdung zu sprechen.
- **G 0.38 Missbrauch personenbezogener Daten:** Diese Problematik stellt hinsichtlich BYOD eine **direkte** Gefährdung dar. Da bei BYOD möglicherweise auch Zugriff auf personenbezogene Daten der Institution besteht, müssen diese vor unbefugtem Zugriff oder vorsätzlicher Weitergabe geschützt werden. Andersherum muss auch der Mitarbeiter vor Missbrauch seiner personenbezogenen Daten geschützt werden.
- **G 0.39 Schadprogramme:** Schadhafte Software wie Viren, Würmer oder Trojaner stellen eine **indirekte** Gefährdung für BYOD dar. Aufgrund der erhöhten Gefährdung durch den Einsatz in privaten Infrastrukturen und öffentlichen Netzen, sollte dieser Punkt gegenüber der Standardbehandlung in den vorhandenen Bausteinen ggf. noch um zusätzliche Aspekte erweitert werden.
- **G 0.40 Verhinderung von Diensten (Denial of Service):** Ein Ausfall von Diensten stellt eine **indirekte** Bedrohung für BYOD dar. Eine gut konfigurierte Firewall etwa kann DoS-Angriffe (z.B. durch Anomalieerkennung) verhindern.
- **G 0.41 Sabotage:** Mutwillige Manipulation von Komponenten einer Institution kann eine **indirekte** Gefährdung für BYOD darstellen, sofern diese Komponenten für die BYOD-Kommunikation von Nöten sind.

- **G 0.42 Social Engineering:** Aufgrund der größeren Verantwortung des Mitarbeiters im Zusammenhang mit BYOD, ist die Beeinflussung der Handlungen des Mitarbeiters eine **direkte** Gefährdung für BYOD.

- **G 0.43 Einspielen von Nachrichten:** Die Manipulation des Datenstroms im Zuge einer Kommunikation durch Replay-Attacke[26] oder Man-in-the-Middle-Attacke[27] ist eine **indirekte** Bedrohung der BYOD-Kommunikation.

- **G 0.44 Unbefugtes Eindringen in Räumlichkeiten:** Bei Einbrüchen in Räumlichkeiten können auch Geräte oder Informationen entwendet werden, die mit der BYOD-Kommunikation im Zusammenhang stehen. Diese Bedrohung ist deshalb als **indirekte** Gefährdung einzuordnen.

- **G 0.45 Datenverlust:** Ein Ereignis, das zum Verlust von Daten führt, ist grundsätzlich problematisch sofern diese Daten nicht bereits gesichert werden konnten. Hinsichtlich BYOD handelt es sich hier oftmals um mobile Geräte, die Daten bei temporär fehlender Internetverbindung nicht immer sofort synchronisieren können. In diesem Fall bedeutet dies eine **indirekte** Gefährdung.

- **G 0.46 Integritätsverlust schützenswerter Informationen:** Integrität beispielsweise hinsichtlich der Datenübertragung ist ein wichtiger Aspekt für BYOD und ein Verlust ebendieser eine **indirekte** Gefährdung.

- **G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe:** Die Vielzahl von Anwendungsformen bei BYOD-Geräten birgt die Gefahr, dass Angriffe mit anderer Ausrichtung plötzlich eine größere Gefährdung bedeuten. Diese Gefährdung ist als **direkt** einzustufen.

Die Bewertung der elementaren Gefährdungen und die Identifizierung vieler Punkte als **indirekt** zeigt, dass BYOD grundsätzlich viele Abhängigkeiten aufweist, die jedoch vielfach bereits in anderen Bausteinen berücksichtigt werden. Um hier eine saubere Abgrenzung vorzunehmen, sollte immer auch die Definition von BYOD (vgl. Kap. 5.1.1) hinzugezogen werden. Die elementaren Gefährdungen wurden dann als **direkt** bewertet, wenn Sie diese Besonderheiten von BYOD betreffen.

Eine Auflistung der ausgewählten elementaren Gefährdungen listet Tabelle 5.3.

[26] Wiedereinspielen von Nachrichten

[27] Einschalten in den Datenstrom und Vermittlung zwischen zwei Teilnehmern, so dass diese davon ausgehen, direkt miteinander zu kommunizieren

Tabelle 5.3: Auf BYOD zutreffende elementare Gefährdungen

	Gefährdung	Grundwert
G 0.14	Ausspähen von Informationen/Spionage	C
G 0.15	Abhören	C
G 0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	C, A
G 0.17	Verlust von Geräten, Datenträgern und Dokumenten	C, A
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A
G 0.19	Offenlegung schützenswerter Informationen	C
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	C, I, A
G 0.21	Manipulation von Hard und Software	C, I, A
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A
G 0.27	Ressourcenmangel	A
G 0.36	Identitätsdiebstahl	C, I, A
G 0.37	Abstreiten von Handlungen	C, I
G 0.38	Missbrauch personenbezogener Daten	C, I
G 0.42	Social Engineering	C, I
G 0.47	Schädliche Seiteneffekte IT-gestützter Angriffe	C, I, A

5.3.2 Ermittlung zusätzlicher Gefährdungen

Im nächsten Schritt werden weitere spezifische Gefährdungen gesucht, die die elementaren Gefährdungen konkretisieren oder über diese hinausgehen. Besonderes Augenmerk wird hier auf die Praxisrelevanz gelegt. Aufgenommen werden nur die Gefährdungen, die im Kontext realistisch sind. Relevanz liegt weiterhin vor, wenn die Gefährdung zu einem nennenswerten Schaden führen könnte.

Vorschläge möglicher spezifischer Gefährdungen, die noch nicht ausreichend berücksichtigt sind:

G z.1 Vermischung privater und beruflicher Daten
Zielobjekte: Lokale Endgeräte (LD), Mobile Endgeräte (MD)
Wenn auf einem Gerät sowohl private als auch berufliche Informationen gespeichert werden, besteht die Gefahr, dass diese Informationen nicht ausreichend voneinander getrennt sind. Dies geschieht beispielsweise durch Programme, die vollständigen Zugriff auf das Adressbuch anfordern. Sollten hier auch institutionelle Informationen betroffen sein, hat dies datenschutzrechtliche Relevanz.

G z.2 Unzureichende Administrationsmöglichkeiten für institutionellen Einsatz
Zielobjekte: Mobile Endgeräte (MD)
Mobile Endgeräte sind im Hinblick auf die Konfigurationsmöglichkeiten zumeist für den Consumer-Bereich vorgesehen und bieten von Hause aus keine erweiterten Optionen wie sie im Unternehmensbereich benötigt werden. Ein einfaches Beispiel ist der explizite Nutzungsausschluss von Systemapplikationen wie Bildschirmfotos.

G z.3 Fehlende Rechtssicherheit im Umgang mit BYOD
Zielobjekte: Nutzung (LU, OU, RU)
Wenn mit BYOD neu auftretende Rechtsfragen nicht ausreichend geregelt sind, kann es im späteren Betrieb zu Irritationen über Rechte und Pflichten kommen. Dies gilt zum Beispiel für die Frage, ob die Institution das Recht hat, das Gerät im Falle eines Verlusts aus der Ferne zu löschen.

G z.4 Fehlende Regelung zu Arbeitszeiten mit BYOD
Zielobjekte: Nutzung (LU, OU, RU)
Durch BYOD gewinnt der Arbeitnehmer zwar an Flexibilität hinsichtlich seiner Arbeitszeit, gleichzeitig birgt jedoch die ständige Erreichbarkeit auch Gefahren. Die Institution verliert ihrerseits Kontrolle darüber, wann der Mitarbeiter arbeitet und wann nicht. Mit Berücksichtigung der möglichen Anrechnung als Arbeitszeit, sobald die Institution eine Bereitschaft aktiv einfordert, sollten bereits im Vorfeld entsprechende Regelungen stattfinden.

G z.5 Fehlende Softwarelizenzen für den BYOD-Einsatz
Zielobjekte: Endgeräte (LD, MD)
Wird institutionelle Software auf dem privaten Endgerät genutzt, so besteht die Möglichkeit, dass Software eingesetzt wird, die in diesem Kontext lizenzrechtlich nicht ausreichend abgesichert ist. In gleicher Weise gilt dies auch für privat erworbene Software/Apps, die durch den Arbeitnehmer für dienstliche Zwecke genutzt werden könnte. Dies kann für den Mitarbeiter als auch die Institution rechtliche Schwierigkeiten und damit verbundene Kosten nach sich ziehen.

G z.6 Fehlende Anpassung an neue Gerätegenerationen
Zielobjekte: Endgeräte (LD, MD), Unternehmensserver (CS), Administrationsserver (AS)
Der mögliche Wunsch der Arbeitnehmer nach Nutzung aktueller Gerätegenerationen, birgt die Gefahr, dass der IT-Betrieb nicht über das notwendige Fachwissen verfügt und eine sichere Integration nicht in jedem Fall gewährleisten kann. Die Unterstützung aktueller Geräte steigert aber andererseits auch die Attraktivität für die Mitarbeiter. Falls beispielsweise Gerätetypen über neuartige (biometrische) Authentifizierungs-Möglichkeiten oder neue Hardwareschnittstellen verfügen, so kann deren Wirksamkeit ohne entsprechendes Fachwissen nur eingeschränkt beurteilt werden.

G z.7 Ungeregeltes Einspielen von Updates auf BYO-Geräten
Zielobjekte: Endgeräte (LD, MD)
Grundsätzlich ist es empfehlens- und wünschenswert ein BYO-Gerät auf dem aktuellen Softwarestand zu halten. Da das BYO-Gerät Eigentum des Mitarbeiters ist, hat er in der Regel auch umfangreiche Rechte auf diesem. Während auf institutseigenen Geräten die Administratoren entscheiden ob ein Softwareupdate installiert wird, so liegt dies auf einem BYO-Gerät standardmäßig in der Verantwortung des Mitarbeiters. Wenn der Mitarbeiter beispielsweise ein Update unmittelbar nach Erscheinen installiert, welches zu Inkompatibilitäten mit den institutionellen Anwendungen führt, kann dies zu einem Problem hinsichtlich der Verfügbarkeit führen. Vereinzelt sind Updates auch generell fehlerhaft und werden kurz nach dem Erscheinen wieder zurückgenommen. Eine IT-Administration wartet deshalb vor der Installation eines Updates in der Produktionsumgebung ggf. noch bzw. testet dieses vorab in einer Simulationsumgebung. Andererseits kann es jedoch auch problematisch sein, wenn der Mitarbeiter, etwa wegen der Inkompatibilität mit vorhandener Software, auf neue Updates verzichtet.

G z.8 Automatisierte Synchronisation mit ungeeigneten Cloud-Diensten
Zielobjekte: Endgeräte (LD, MD)
Die umfangreicheren Rechte, die ein BYOD-Mitarbeiter auf seinem Gerät hat, geben ihm auch die Möglichkeit, Informationen mit externen Cloud-Diensten zu synchronisieren. Standardmäßig besteht dabei die Gefahr, dass dies auch institutionelle Informationen betreffen könnte und die Institution die Kontrolle darüber verliert, wo ihre Informationen gespeichert werden.

G z.9 Ungeregelte Aussonderung von BYO-Geräten
Zielobjekte: Endgeräte (LD, MD)
Eine ungeregelte Aussonderung eines BYO-Geräts, bei dem etwa durch einen Defekt keine Löschung (Corporate-Wipe) mehr möglich war, stellt gegebenenfalls eine Gefahr für noch auf dem Gerät gespeicherte institutionelle Informationen dar.

G z.10 Nicht oder unzureichend an BYOD angepasster Support
Zielobjekte: Endgeräte (LD, MD)
Die Möglichkeit zum zeit- und ortsunabhängigen Arbeiten mit BYOD stellt neue Herausforderungen an den Support der Institution. Es reicht ggf. nicht mehr aus einen Helpdesk während der Arbeitszeiten anzubieten, da BYOD-Mitarbeiter unter Umständen auch zu anderen Zeiten ein akutes Problem haben können, welches bei falscher Handhabung auch institutionelle Informationen gefährden kann.

G z.11 Nutzung von BYO-Geräten durch Dritte
Zielobjekte: Endgeräte (LD, MD)
Haben Familienangehörige oder Freunde Zugang zum BYO-Gerät, können durch unsachgemäße Benutzung des Gerätes die institutionellen Informationen gefährdet werden.

5.3.3 Zuordnung identifizierter Gefährdungen zu Zielobjekten

Aus der Ermittlung der relevanten elementaren Gefährdungen und den zusätzlichen Gefährdungen lässt sich in Kombination mit den Zielobjekten zu BYOD die in Tabelle 5.4 dargestellte Zuordnung ableiten.

Tabelle 5.4: Zuordnung von Gefährdungen zu Zielobjekten

	LD	MD	LU	OU	RU	CC	PS	CS	AS
G 0.14			X	X	X				
G 0.15			X	X	X				
G 0.16		X							
G 0.17		X							
G 0.18						X	X	X	X
G 0.19			X	X	X				
G 0.20	X	X							
G 0.21	X	X					X	X	X
G 0.26	X	X					X	X	X
G 0.27	X	X					X	X	X
G 0.36						X	X	X	X
G 0.37							X	X	X
G 0.38			X	X	X				
G 0.42							X	X	X
G 0.47			X	X	X	X	X	X	X
G z.1	X	X	X	X	X				
G z.2		X							
G z.3			X	X	X				
G z.4			X	X	X				
G z.5	X	X							
G z.6	X	X						X	X
G z.7	X	X							
G z.8	X	X							
G z.9	X	X							
G z.10	X	X							
G z.11	X	X							

5.4 Risikoeinstufung

Zur weiteren Einschätzung ist es notwendig die identifizierten Gefährdungen hinsichtlich ihrer **Eintrittshäufigkeit** und ihrer potenziellen **Schadenshöhe** zu klassifizieren.
Da eine quantitative Einschätzung nur schwer realisierbar ist, wird hier eine qualitative Bewertung vorgenommen. Entsprechend der gängigen Praxis [vgl. 11, S.26] werden die in Tabelle 5.5 und Tabelle 5.6 aufgelisteten Stufen festgelegt [vgl. 11, S.27].

Tabelle 5.5: Kategorisierung von Eintrittshäufigkeiten

Eintrittshäufigkeit	Beschreibung
selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Tabelle 5.6: Kategorisierung von Schadensauswirkungen

Schadenshöhe	Schadensauswirkungen
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Die Nutzung von Eintrittshäufigkeiten und Schadensauswirkungen entlang den Achsen einer Matrix ergibt die in Abbildung 5.7 dargestellte Anordnung [vgl. 11, S.27]. Die Bedeutung der verwendeten Risikokategorien [vgl. 11, S.28] wird in Tabelle 5.8 erläutert.

Tabelle 5.8: Risikokategorien

Risikokategorien	Beschreibung
gering	Das Risiko ist überschaubar und kann, unter fortgesetzter Beobachtung der Gefährdung, akzeptiert werden.
mittel	Das Risiko ist in einem nicht akzeptablen Maß vorhanden und sollte behandelt werden.
hoch	Das Risiko hat ein beträchtliches Maß und kann eine Bedrohung für die Institution darstellen.

Im weiteren Vorgehen werden diese Einstufungen auf die identifizierten Gefährdungen angewendet.

G 0.14 Ausspähen von Informationen/Spionage		
Betroffene Zielobjekte: Nutzung (LU, OU, RU)	Beeinträchtigte Grundwerte: Vertraulichkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**

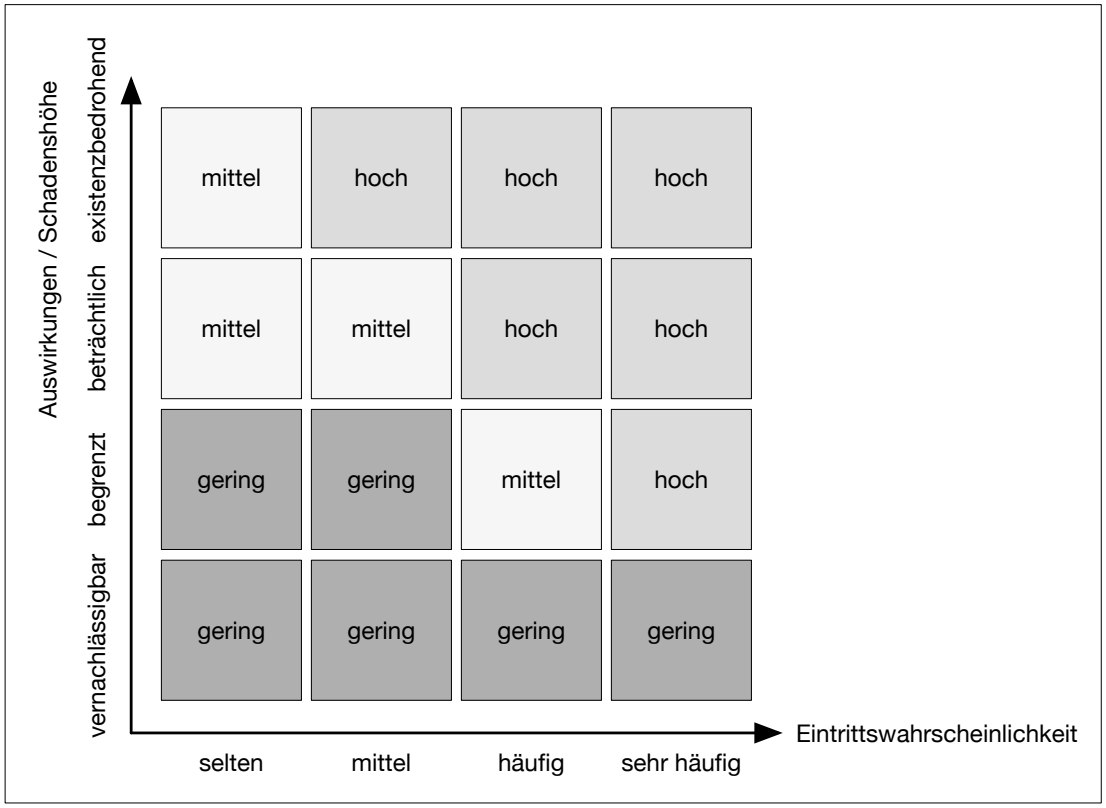

Abbildung 5.7: Risikomatrix

G 0.15 Abhören		
Betroffene Zielobjekte: Nutzung (LU, OU, RU)		Beeinträchtigte Grundwerte: Vertraulichkeit
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**

G 0.16 Diebstahl von Geräten, Datenträgern und Dokumenten		
Betroffene Zielobjekte: Mobile Endgeräte (MD)		Beeinträchtigte Grundwerte: Vertraulichkeit, Verfügbarkeit
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **mittel**

G 0.17 Verlust von Geräten, Datenträgern und Dokumenten		
Betroffene Zielobjekte: Mobile Endgeräte (MD)	Beeinträchtigte Grundwerte: Vertraulichkeit, Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **mittel**

G 0.18 Fehlplanung oder fehlende Anpassung		
Betroffene Zielobjekte: Kommunikationsverbindung (CC), Server (PS, CS, AS)	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: sehr häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**

G 0.19 Offenlegung schützenswerter Informationen		
Betroffene Zielobjekte: Nutzung (LU, OU, RU)	Beeinträchtigte Grundwerte: Vertraulichkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **mittel**

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle		
Betroffene Zielobjekte: Endgeräte (LD, MD)	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: selten	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**

G 0.21 Manipulation von Hard- und Software		
Betroffene Zielobjekte: Endgeräte (LD,MD), Kommunikationsverbindung (CC), Server (PS,CS,AS)	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: selten	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**

G 0.26 Fehlfunktion von Geräten oder Systemen		
Betroffene Zielobjekte: Endgeräte (LD,MD), Kommunikationsverbindung (CC), Server (PS,CS,AS)	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: selten	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **gering**

G 0.27 Ressourcenmangel		
Betroffene Zielobjekte: Endgeräte (LD,MD), Kommunikationsverbindung (CC), Server (PS,CS,AS)	Beeinträchtigte Grundwerte: Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **mittel**

G 0.36 Identitätsdiebstahl		
Betroffene Zielobjekte: Kommunikationsverbindung (CC), Server (PS,CS,AS)	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: selten	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**

G 0.37 Abstreiten von Handlungen		
Betroffene Zielobjekte: Server (PS,CS,AS)	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: selten	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**

G 0.42 Social Engineering		
Betroffene Zielobjekte: Server (PS,CS,AS)	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**

G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe		
Betroffene Zielobjekte: Nutzung (LU,OU,RU)	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **mittel**

G z.1 Vermischung privater und beruflicher Informationen		
Betroffene Zielobjekte: Endgeräte (LD, MD)	Beeinträchtigte Grundwerte: Vertraulichkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: sehr häufig	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **hoch**

G z.2 Unzureichende Administrationsmöglichkeiten für institutionellen Einsatz		
Betroffene Zielobjekte: Mobile Endgeräte (MD)	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **mittel**

G z.3 Fehlende Rechtssicherheit im Umgang mit BYOD		
Betroffene Zielobjekte: Nutzung (LU, OU, RU)	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: sehr häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**

G z.4 Fehlende Regelung zu Arbeitszeiten mit BYOD		
Betroffene Zielobjekte: Nutzung (LU, OU, RU)	Beeinträchtigte Grundwerte: Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: sehr häufig	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **hoch**

G z.5 Fehlende Softwarelizenzen für den BYOD-Einsatz		
Betroffene Zielobjekte: Endgeräte (LD, MD)	Beeinträchtigte Grundwerte: Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**

G z.6 Fehlende Anpassung an neue Gerätegenerationen		
Betroffene Zielobjekte: Unternehmensserver (CS), Administrationsserver (AS)	Beeinträchtigte Grundwerte: Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**

G z.7 Ungeregeltes Einspielen von Updates auf BYO-Geräten		
Betroffene Zielobjekte: Endgeräte (LD, MD)	Beeinträchtigte Grundwerte: Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: selten	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **gering**

G z.8 Automatisierte Synchronisation mit ungeeigneten Cloud-Diensten		
Betroffene Zielobjekte: Endgeräte (LD, MD)	Beeinträchtigte Grundwerte: Vertraulichkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **mittel**

G z.9 Ungeregelte Aussonderung von BYO-Geräten		
Betroffene Zielobjekte: Endgeräte (LD, MD)	Beeinträchtigte Grundwerte: Vertraulichkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**

G z.10 Nicht oder unzureichend an BYOD angepasster Support		
Betroffene Zielobjekte: Endgeräte (LD, MD)	Beeinträchtigte Grundwerte: Verfügbarkeit, Vertraulichkeit, Integrität	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**

G z.11 Nutzung von BYO-Geräten durch Dritte		
Betroffene Zielobjekte: Endgeräte (LD, MD)	Beeinträchtigte Grundwerte: Vertraulichkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**

5.5 Ermittlung von Anforderungen

In welchem Maße Risiken behandelt werden, hängt vom Risikoappetit der Institution ab. Zum Management der Risiken sind folgende Behandlungsoptionen definiert:

- **A: Risikovermeidung:** Durch Ausschluss der Risikoursache
- **B: Risikoreduktion:** Durch Modifikation der Umstände, die zur Risikoeinstufung beigetragen haben
- **C: Risikotransfer:** Durch (teilweise) Übertragung an einen Dritten

Eine mögliche vierte Option der Risikoakzeptanz ist an dieser Stelle nicht vorgesehen.

Die Anforderungen, die an die Institution gestellt werden, können an unterschiedlichen Punkten ansetzen:

- **Verschlüsselung:** Es muss eine gesichterte Kommunikation zwischen BYO-Gerät und Institutionsservern sichergestellt werden. Auf dem BYO-Gerät muss eine sichere Speicherung der Unternehmensdaten gewährleistet und die Daten vor Schadsoftware geschützt werden [vgl. 49, S.3].
- **Datenschutz:** Als verantwortliche Stelle ist eine Institution Datenschutzrechtlich für die Verarbeitung von personenbezogenen, dienstlichen Daten zuständig. Dies gilt auch dann, wenn die Daten auf dem mobilen Endgerät des Mitarbeiters verarbeitet werden (vgl. § 3 Abs. 7 BDSG). Die Institution hat in diesem Fall die Pflicht, die gesetzlichen Anforderungen an den Datenschutz

und die Datensicherheit zu gewährleisten (§ 9 Satz 1 BDSG). Weiter muss sie gewährleisten, dass die Nutzung des Datenverarbeitungssystems durch Unbefugte ausgeschlossen ist und Mitarbeiter nur im Rahmen bestehender Berechtigungen auf Daten zugreifen können. Daten müssen vor Zerstörung und Verlust geschützt, sowie Vertraulichkeit und Integrität gewährleistet sein. Es muss überdies eine Protokollierung stattfinden ob und von wem Daten in das Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind [vgl. 49, S.3].

- **Organisatorische Regelungen:** Die Besitzverhältnisse hinsichtlich eines BYO-Gerätes haben zur Folge, dass die Institution nicht nach Belieben über das Gerät disponieren kann. Deshalb ist eine Regelung über die (Mitwirkungs-)Pflichten des Mitarbeiters im Zusammenhang mit BYOD notwendig [vgl. 49, S.4]. Dies könnten in Form eine zu unterzeichnenden Nutzungsvereinbarung realisiert werden. Weiterhin ist der Mitarbeiter im Betrieb mehr auf sich selber gestellt, so dass er über ein zusätzliches Wissen im Umgang (z.B. in welchen Umgebungen kann ich sicher arbeiten) verfügen sollte. Dieses Wissen sollte über Hinweise oder (Online-)Schulungen vermittelt werden.

- **Vereinfachung der Administration:** Da es bei Consumer-Geräten an erweiterten Konfigurationsmöglichkeiten (wie Institutionen sie ggf. benötigen) mangelt, sollte zur zentralen Verwaltung der Geräte eine Management-Lösung zum Einsatz kommen. Diese Software-Lösungen (vgl. Kap. 2.3.6 und 4.4) gibt es in unterschiedlichen Umfängen und ermöglichen die zentralisierte Konfiguration, Verwaltung und Löschung aus der Ferne.

- **Datentrennung:** Die Trennung der beruflich genutzten Informationen von den privaten Daten ist aus folgenden Gründen unbedingt erforderlich:

  - Berufliche Daten könnten sonst im unerlaubten Kontext eingesetzt werden. Beispielsweise greifen Programme auf das Adressbuch zu und ohne weitere Lösung lassen sich die dort gespeicherten Kontakte nicht trennen.

  - Berufliche Daten dürfen aus lizenzrechtlichen Gründen nur mit Programmen bearbeitet werden können, die für die betriebliche Verwendung freigegeben sind.

  - Berufliche Daten sollten sich getrennt von privaten Informationen löschen lassen.

  - Berufliche Daten sollten sich in nativer Umgebung nutzen lassen. Trotz Trennung ist es für die Akzeptanz der Benutzer wichtig, dass beispielsweise das gewohnte E-Mail-Programm auch im beruflichen Kontext eingesetzt werden kann.

Eine Datentrennung in der beschriebenen Art lässt sich auf technischer Ebene mit geeigneten Management-Lösungen (MAM oder EMM/UEM) in Form eines Containers realisieren.

Zur Behandlung der identifizierten Gefährdungen werden mit Hilfe der beschriebenen Anforderungen entsprechende Lösungsempfehlungen formuliert:

G 0.14 Ausspähen von Informationen/Spionage		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Nutzung (LU,OU,RU)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Sensibilisierung durch Schulung oder Hinweise in Nutzungsvereinbarung dafür, ergänzende Hardware zur Erschwerung (z.B. Schutzfolien mit Blickschutz) zu verwenden.

G 0.15 Abhören		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Nutzung (LU,OU,RU)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Automatischer Einsatz einer (optional nur auf die App bezogenen) VPN-Verbindung um den Datenstrom gegen Abhören zu sichern.

G 0.16 Diebstahl von Geräten, Datenträgern und Dokumenten		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Mobile Endgeräte (MD)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Als proaktive Maßnahme sollte der Nutzer in den Nutzungsbedingungen auf die Einhaltung bestimmter Sicherheitsrichtlinien hin verpflichtet werden. Beispielsweise das Tablet nicht unbeaufsichtigt liegen lassen oder das Smartphone nicht in der Gesäßtasche transportieren.

G 0.17 Verlust von Geräten, Datenträgern und Dokumenten		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Mobile Endgeräte (MD)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Um auf den Verlust eines Gerätes angemessen reagieren zu können, wird im Vorfeld ein Notfallplan benötigt: Um ein verlorenes Gerät reaktiv wieder auffinden zu können, sollte eine Ortungsfunktion aktiviert werden. Gleichzeitig sollten die entsprechenden Zugänge zu Unternehmensressourcen für dieses Gerät gesperrt werden. Für den Fall, dass das Gerät nicht auffindbar ist, muss zusätzlich die Möglichkeit der Remote-Löschung von Unternehmensdaten verfügbar sein.

G 0.18 Fehlplanung oder fehlende Anpassung		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Kommunikationskanal (CC), Server (PS,CS,AS)	hoch mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Die mit dem Thema BYOD betreuten Administratoren sollten regelmäßige Fortbildungen oder Schulungen besuchen können, sowie die Ressourcen für regelmäßige Planung von Weiterentwicklungen zur Verfügung gestellt bekommen. Weiter bedarf es einer Richtlinie zum Thema BYOD, in der die essentiellen organisatorischen, technischen und rechtlichen Regelungen berücksichtigt werden.

G 0.19 Offenlegung schützenswerter Informationen		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Nutzung (LU,OU,RU)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: In Punkto eines möglichen Passwortverlustes könnte durch Nutzung einer Zwei-Faktor-Authentifizierung und/oder biometrischer Verfahren (Fingerabdruck/-Gesichtsscanner), wie sie vermehrt auch schon in Consumergeräten zur Verfügung stehen, die Sicherheit erhöht werden. Einsatz einer Management-Lösung zur automatischen Verschlüsselung der geschäftlichen Daten (Container).

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD,MD)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Durch Einsatz einer Management-Lösung kommen nur sogenannte gemanagte Programme in den Kontakt mit den Unternehmensdaten. Diese verfügt weiterhin über Möglichkeiten modifizierte Betriebssysteme (Jailbreak, gerootet) zu erkennen. Bei modernen Computern, die mit einem UEFI ausgestattet sind, kann dieses (bei aktiviertem User-Mode) im SecureBoot-Modus betrieben werden. Dadurch wird nur Code ausgeführt, der über eine Signatur entspricht. Smartphones verfügen (je nach Modell) standardmäßig über Mechanismen, die ebenfalls eine sichere Bootkette garantieren.

G 0.21 Manipulation von Hard- und Software		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD,MD), Server (PS,CS,AS)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Beschränkung auf bestimmte Systeme, die aufgrund ihrer Architektur besser gegen Modifikationen geschützt sind. Ein Beispiel wären iOS-basierte Geräte deren Sicherheitsmechanismen sich nur über einen so genannten Jailbreak aufheben lassen. Das Vorhandensein solcher Hacks lässt sich aus der Ferne über ein Managementsystem (MDM) feststellen.

G 0.26 Fehlfunktion von Geräten und Systemen		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD,MD), Server (PS,CS,AS)	gering mit erg. Maßnahme: gering	C: Risikotransfer: Da sich das Gerät im Besitz des Mitarbeiters befindet, hat dieser Fürsorge dafür zu tragen, dass dieses ordnungsgemäß funktioniert. Dies sollte in der Nutzungsvereinbarung fixiert sein. Der Vielzahl an möglichen Fehlfunktionen könnte hinsichtlich Detektion standardisiert nur mit unverhältnismäßig hohem Support-Aufwand begegnet werden.

G 0.27 Ressourcenmangel		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD,MD), Server (PS,CS,AS)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Multiplikatoren sorgen hinsichtlich des Personals dafür, dass Spezialwissen nicht auf einzelne Personen beschränkt bleibt. Auf Geräteebene müssen notwendige Systemvoraussetzungen benannt werden, die regelmäßige Anpassung erhalten.

G 0.36 Identitätsdiebstahl		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Mobile Endgeräte (MD)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Einsatz eines Mechanismus, der unsichere Passwörter vermeidet und regelmäßige Erneuerung verlangt. Einsatz von Single-Sign-On um die wiederholte Eingabe von Passwörtern zu vermeiden. Aktivierung von Zwei-Faktor-Authentifizierung um relevante Einstellungen zusätzlich zu schützen.

G 0.37 Abstreiten von Handlungen		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Mobile Endgeräte (MD)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Durch Einsatz von Signaturen bzw. Zertifikaten können Handlungen eindeutig einer bestimmten Kennung zugeordnet werden. Das verstärkte Risiko durch die freiere Arbeitsweise im Zusammenhang mit BYOD kann dadurch gemindert werden.

G 0.38 Missbrauch personenbezogener Daten		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Mobile Nutzung (MU), Remote Nutzung (RU)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Trennung privater Daten der Mitarbeiter von den institutionellen Informationen durch Einsatz einer Container-Lösung, die in der Regel Bestandteil einer Management-Lösung (MAM, EMM, UEM) ist.

G 0.42 Social Engineering		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Server (PS,CS,AS)	hoch mit erg. Maßnahme: normal	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Social Engineering kann in verschiedenen Ausprägungen stattfinden (vgl. Kap.3.1.2). Risikoreduktion findet vor allem durch Sensibilisierung der Mitarbeiter (Awareness) statt. Wenn dieser etwa durch Schulungen und Verhaltenshinweisen (z.B. mittels Richtlinie) darauf hingewiesen wird, Vorsicht hinsichtlich solcher E-Mails, Dateianhängen, sozialen Netzwerken aber auch gegenüber Fremden zu haben, ist das Risiko reduzierbar.

G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Mobile Endgeräte (MD)	mittel mit erg. Maßnahme: gering	B: Einsatz von Black-/Whitelists hinsichtlich erlaubter App-Installationen reduzieren mögliche Wechselwirkungen auf dem BYO-Gerät.

G z.1 Vermischung privater und beruflicher Informationen		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD, MD)	hoch mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Zur Reduzierung des Risikos wird eine Management-Lösung mit Container-Funktion eingesetzt. Dadurch werden die beruflichen Daten in einem eigenen Bereich gekapselt und lassen sich auch nur mit ausgewählten Programmen öffnen. Weiter ist diese Aufteilung Voraussetzung für eine gezielte Löschung der institutionellen Daten ohne Auswirkungen auf private Informationen.

G z.2 Unzureichende Administrationsmöglichkeiten für institutionellen Einsatz		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Mobile Endgeräte (MD)	mittel mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Um das Risiko zu reduzieren, sollen nur Endgeräte bestimmter Plattformen sowie (Mindest-)Betriebssystem-Versionen zugelassen werden. Dadurch beschränken sich die Lösungen zur Administration auf weniger Zielsysteme wodurch sich der Aufwand reduziert. Weiter kommt eine Management-Lösung zum Einsatz, welche die Administrationsmöglichkeiten des Herstellers erweitert und vereinfacht.

G z.3 Fehlende Rechtssicherheit im Umgang mit BYOD		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Nutzung (LU, OU, RU)	hoch mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Die Mitarbeiter bekommen vor der Freischaltung eine schriftliche Nutzungsvereinbarung mit rechtlichen Hinweisen, deren Kenntnis sie durch Unterzeichnung bestätigen müssen. Zusätzlich können freiwillige oder verpflichtende Schulungsveranstaltungen zur Sensibilisierung für die relevanten Themen angeboten werden und zusätzlich dazu beitragen, Verständnis für die Maßnahmen der Institution zu schaffen.

G z.4 Fehlende Regelung zu Arbeitszeiten mit BYOD		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Nutzung (LU, OU, RU)	hoch mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Die Mitarbeiter werden in der Nutzungsvereinbarung dazu verpflichtet ihre Arbeitszeiten mit den Kernarbeitszeiten der Institution abzustimmen. Zusätzlich könnten bestimmte Dienste zu ausgewählten Zeiten (nachts, am Wochenende/Feiertagen oder zu Urlaubszeiten des Mitarbeiters) temporär deaktiviert werden.

G z.5 Fehlende Softwarelizenzen für den BYOD-Einsatz		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD, MD)	hoch mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Zur Reduktion des Risikos werden die Mitarbeiter in einer Nutzungsvereinbarung darauf hingewiesen, dass sie im betrieblichen Rahmen nur die Software nutzen dürfen, die ihnen seitens der Institution zur Verfügung gestellt wurde. Diese Vorgabe könnte in einem weiteren Schritt auf technischer Ebene durch den Einsatz einer Management-Lösung mit Container-Funktionalität sichergestellt werden. Dadurch können institutionelle Informationen nur noch mit freigegebenen (gemanagten) Programmen weiter verarbeitet werden.

G z.6 Fehlende Anpassung an neue Gerätegenerationen		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD, MD), Server (CS, AS)	gering mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Reduzierung des Risikos durch Einsatz einer Geräte-Freigabeliste: Neu auf dem Markt erschienene Geräte bzw. Betriebssysteme werden erst verzögert nach einem Test stufenweise zur Nutzung freigegeben. Bestimmte Dienste werden auf älteren Geräten bzw. Betriebssystemen nach vorgegeben Zeiträumen deaktiviert. Zusätzlich regelmäßige Fortbildungen der betroffenen Mitarbeiter des IT-Betriebs.

G z.7 Ungeregeltes Einspielen von Updates auf BYO-Geräten		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD, MD)	gering mit erg. Maßnahme: gering	A: Risikovermeidung durch ergänzende Sicherheitsmaßnahme: Die Administration übernimmt die Softwareaktualisierung durch zentralisiertes Einspielen über eine Management-Lösung.

G z.8 Automatisierte Synchronisation mit ungeeigneten Cloud-Diensten		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD, MD)	mittel mit erg. Maßnahme: gering	A: Risikovermeidung durch ergänzende Sicherheitsmaßnahme: Deaktivierung der Nutzung von Cloud-Diensten über eine Management-Lösung. B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Gesonderte Verschlüsselung institutioneller Informationen im Container.

G z.9 Ungeregelte Aussonderung von BYO-Geräten gefährdet institutionelle Informationen		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD, MD)	hoch mit erg. Maßnahme: gering	A: Risikovermeidung durch ergänzende Sicherheitsmaßnahme: Nutzung von On-the-Fly-Verschlüsselung des Betriebssystems wie BitLocker (Windows) bzw. FileVault (macOS). Auf iOS-Geräten ist automatisch eine Verschlüsselung aktiviert, auf Android ist diese optional nutzbar. Voraussetzung ist die Löschung vor Aussonderung! B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Aufnahme entsprechender Verhaltenshinweise in die Benutzerrichtlinie: Geräte dürfen nur nach Absprache mit der Administration weitergegeben bzw. veräußert werden.

G z.10 Nicht oder unzureichend an BYOD angepasster Support		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD, MD)	hoch mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Weiterbildung der Support-Mitarbeiter zu BYOD-spezifischen Themen. Ergänzung des Helpdesks durch einen Online-Support zur Selbsthilfe rund um die Uhr.

G z.11 Nutzung von BYO-Geräten durch Dritte		
Zielobjekt	Kategorie	Risikobehandlungsoptionen
Endgeräte (LD, MD)	hoch mit erg. Maßnahme: gering	B: Risikoreduktion durch ergänzende Sicherheitsmaßnahme: Ausschluss der Weitergabe des BYO-Gerätes an Dritte mittels Richtlinie. Nutzung einer biometrischen Authentifizierung, sofern verfügbar.

5.6 Konsolidierung des Sicherheitskonzepts

Im Rahmen der Konsolidierung werden die ergänzenden Maßnahmen hinsichtlich folgender Kriterien [11, S.39] untersucht, bewertet und ggf. modifiziert:

- **Eignung** der Sicherheitsmaßnahmen zur Abwehr der Gefährdungen: Die empfohlenen Sicherheitsmaßnahmen können das Risiko, das von den Gefährdungen ausgeht, verringern.

- **Zusammenwirken** der Sicherheitsmaßnahmen: Die empfohlenen Sicherheitsmaßnahmen finden auf organisatorischer, Applikations- und Geräteebene statt und stehen nicht im Konflikt zueinander.

- **Benutzerfreundlichkeit** der Sicherheitsmaßnahmen: Grundsätzlich hat die Reduzierung des Risikos Priorität und dies erfordert auch Einschränkungen in der Freiheit des BYOD-Nutzers. Benutzerfreundlichkeit wird vor allem hinsichtlich der technischen Lösung (Management-Lösung ggf. mit Container) erwartet. Dies ist dadurch gegeben, dass es beispielsweise keiner komplexen Einrichtung durch Dritte bedarf, sondern der Mitarbeiter diese Schritte selber durchführen könnte. Im späteren Betrieb integrieren sich Dienste (E-Mail oder Kontakte) ebenfalls nativ in die gewohnte Programmstruktur ohne aber die Informationen privater und institutioneller Herkunft zu vermischen.

- **Angemessenheit/Qualitätssicherung** der Sicherheitsmaßnahmen: Hinsichtlich der Angemessenheit wirft vor allem die Nutzungsvereinbarung Fragen auf. Notwendig um Rechtssicherheit zu schaffen, sollte seitens der Institution trotzdem darauf geachtet werden, den Mitarbeiter nicht zu stark in seiner Freiheit einzuschränken.

- **Integration** der Inhalte: Das Thema BYOD ist recht weitläufig und eng mit einigen anderen Bausteinen verknüpft. Auch wenn es bisher keinen eigenen Baustein zum Thema gab, so findet BYOD bereits in den Bausteinen *SYS.3.2.1 Allgemeine Smartphones und Tablets* sowie *SYS.3.2.2 Mobile Device Management (MDM)* Erwähnung. Die entsprechenden Einträge sollten angepasst werden.

Bei der Konsolidierung wurde Folgendes festgestellt:

- Das IT-Grundschutz-Kompendium deckt bereits einige, für BYOD identifizierten, Gefährdungen ab. Es fehlt jedoch teilweise an Tiefe für das Szenario des BYOD-Betriebs außerhalb der informationstechnischen Grenzen der Institution. So geben beispielsweise die *Umsetzungshinweise zum Baustein ORP.3*

Sensibilisierung und Schulung[28] umfangreiche Informationen zu möglichen Schulungsinhalten. Ergänzt werden sollten diese jedoch noch um Awareness-Hinweise zum Betrieb im öffentlichen Raum. Hier besteht erhöhte Gefährdung durch Abhören/Abschauen und ein höheres Risiko für Diebstahl/Verlust.

- Aufgrund der vielen Anknüpfungspunkte von BYOD wird das Konzept in den Bausteinen vereinzelt schon erwähnt bzw. bearbeitet. Beispielsweise findet sich in den Umsetzungshinweisen zum Baustein *SYS.3.2.2 Mobile Device Management (MDM)*[29] eine umfangreiche Auflistung von Fragen, ob BYOD für die Institution freigegeben werden kann. Diese Inhalte sollten mit Verweis zum BYOD-Baustein übernommen werden.
- Bei der Ausarbeitung wurde festgestellt, dass zur Erreichung der Ziele schon ab einem sehr geringen Umfang von BYOD der Einsatz einer Management-Lösung zur Erreichung der Schutzziele unabdingbar ist.
- Hinsichtlich der Widersprüchlichkeit von Maßnahmen gibt es eine Einschränkung, die ggf. in Konflikt zueinander steht: Der BYOD-Nutzer sollte grundsätzlich automatisiert sicherstellen, dass die Software auf dem Gerät immer auf dem aktuellen Stand ist. Dies widerspricht der Gefährdung *G.z.7 Ungeregeltes Einspielen von Updates auf BYO-Geräten*. Grundsätzlich sollte dies nur bei einem erhöhten Sicherheitsbedarf in Erwägung gezogen werden und standardmäßig die automatische Installation von Updates präferiert werden.

[28] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/ORP/Umsetzungshinweise_zum_Baustein_ORP_3_Sensibilisierung_und_Schulung.html

[29] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/SYS/Umsetzungshinweise_zum_Baustein_SYS_3_2_2_Mobile_Device_Management_(MDM).html

6 Erstellung des IT-Grundschutz Bausteins

Nachdem im vorherigen Kapitel die Inhalte des Bausteins erarbeitet wurden, so wird in diesem Kapitel die Essenz für die textliche Umsetzung gemäß der Form des BSI aufbereitet. Die Einordnung des Bausteins wird im Bereich *CON: Konzeption und Vorgehensweisen* als Baustein *CON.8 BYOD* empfohlen.

6.1 Beschreibung

CON.8 BYOD

6.1.1 Einleitung

Mobilität und Flexibilität sind, auch bei der IT-Nutzung einer Institution, selbstverständlich geworden. Die Anforderung, unterwegs sicher seine E-Mails oder Termine abzurufen oder auf das Institutionsnetzwerk zugreifen zu können, ist technisch möglich. Zunehmend gewünscht wird in diesem Zusammenhang die kombinierte Nutzung eines IT-Gerätes für berufliche und private Zwecke, wodurch neue Herausforderungen für die Informationssicherheit entstehen. Private und institutionelle Informationen müssen auseinander gehalten sowie unterschiedliche Hardware in den Informationsverbund integriert und verwaltet werden.
Je nach Ausprägung wird in diesem Zusammenhang von Consumerisation oder Bring your own Device (BYOD) gesprochen. Während Consumerisation als Teilmenge von BYOD lediglich die private Nutzung institutionseigener Geräte umfasst, so steht BYOD für den Einsatz von selbstständig angeschafften (ggf. subventionierten) Geräten der Mitarbeiter im privaten und beruflichen Bereich.
Die Anforderungen an die Institution hinsichtlich der Umsetzung sind vielfältig auf organisatorischer, Applikations- und Geräteebene angesiedelt.

6.1.2 Zielsetzung

Ziel des Bausteins ist die Integration von mitarbeitereigenen Geräten, die nicht im Einfluss des Arbeitgebers stehen. Dazu werden typische Gefährdungen aufgezeigt und spezielle Anforderungen an BYOD gestellt.

6.1.3 Abgrenzung

Dieser Baustein konzentriert sich auf die sicherheitstechnischen Besonderheiten, mit denen Institutionen durch die Einführung von BYOD konfrontiert werden. BYOD als Nutzungskonzept erstreckt sich über verschiedene Bereiche mit organisatorischen, technischen und rechtlichen Aspekten. Dadurch sind auch vermehrt Kontaktpunkte mit anderen Bausteinen gegeben, die bei der Umsetzung zu beachten sind.

Sicherheitsanforderungen an die Endgeräte und deren Betriebssysteme werden im vorliegenden Baustein nicht berücksichtigt, sondern sind Bestandteil der jeweiligen Bausteine unter SYS: *IT-Systeme*.

Es wird ferner eine funktionierende Kommunikationsverbindung vorausgesetzt, welche entweder über eine Datenverbindung eines Telekommunikationsdienstleisters hergestellt oder mittels einer WLAN-Verbindung (NET.2.2: *WLAN-Nutzung*) realisiert wird. Zur Absicherung der Verbindung wird zusätzlich auf den Baustein NET.3.3: *VPN* verwiesen.

Organisatorische Grundlagen liefern die Bausteine aus ORP: *Organisation und Personal*.

Die Anforderungen aus dem themenüberschneidenden Baustein SYS.3.2.2 *Mobile Device Management (MDM)* und OPS.1.2.4 *Fernwartung* sind zu beachten.

Weitere, auch für BYOD gültige Aspekte, finden sich in:

- INF.8 *Häuslicher Arbeitsplatz*
- INF.9 *Mobiler Arbeitsplatz*
- OPS.1.2.4 *Telearbeit*
- CON.7 *Informationssicherheit auf Auslandsreisen*

6.2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein CON.8 *BYOD* von besonderer Bedeutung:

6.2.1 Vermischung privater und beruflicher Informationen

Wenn auf einem Gerät sowohl private als auch berufliche Informationen gespeichert werden, besteht die Gefahr, dass diese Informationen nicht ausreichend voneinander getrennt sind. Dies geschieht beispielsweise durch Programme, die vollständigen Zugriff auf das Adressbuch anfordern. Sollten hier auch institutionelle Informationen betroffen sein, hat dies datenschutzrechtliche Relevanz.

6.2.2 Unzureichende Administrationsmöglichkeiten für institutionellen Einsatz

Mobile Endgeräte sind im Hinblick auf die Konfigurationsmöglichkeiten zumeist für den Consumer-Bereich vorgesehen und bieten von Hause aus keine erweiterten Optionen wie sie im Unternehmensbereich benötigt werden. Ein einfaches Beispiel ist der explizite Nutzungsausschluss von Systemapplikationen wie Bildschirmfotos.

6.2.3 Fehlende Rechtssicherheit im Umgang mit BYOD

Wenn mit BYOD neu auftretende Rechtsfragen nicht ausreichend geregelt sind, kann es im späteren Betrieb zu Irritationen über Rechte und Pflichten kommen. Dies gilt zum Beispiel für die Frage, ob die Institution das Recht hat, das Gerät im Falle eines Verlusts aus der Ferne zu löschen.

6.2.4 Fehlende Regelung zu Arbeitszeiten mit BYOD

Durch BYOD gewinnt der Arbeitnehmer zwar an Flexibilität hinsichtlich seiner Arbeitszeit, gleichzeitig birgt jedoch die ständige Erreichbarkeit auch Gefahren. Die Institution verliert ihrerseits Kontrolle darüber, wann der Mitarbeiter arbeitet und wann nicht. Mit Berücksichtigung der möglichen Anrechnung als Arbeitszeit, sobald die Institution eine Bereitschaft aktiv einfordert, sollten bereits im Vorfeld entsprechende Regelungen stattfinden.

6.2.5 Fehlende Softwarelizenzen für den BYOD-Einsatz

Wird institutionelle Software auf dem privaten Endgerät genutzt, so besteht die Möglichkeit, dass Software eingesetzt wird, die in diesem Kontext lizenzrechtlich nicht ausreichend abgesichert ist. In gleicher Weise gilt dies auch für privat erworbene Software/Apps, die durch den Arbeitnehmer für dienstliche Zwecke genutzt werden könnte. Dies kann für den Mitarbeiter als auch die Institution rechtliche Schwierigkeiten und damit verbundene Kosten nach sich ziehen.

6.2.6 Fehlende Anpassung an neue Gerätegenerationen

Der mögliche Wunsch der Arbeitnehmer nach Nutzung aktueller Gerätegenerationen, birgt die Gefahr, dass der IT-Betrieb nicht über das notwendige Fachwissen verfügt und eine sichere Integration nicht in jedem Fall gewährleisten kann. Die Unterstützung aktueller Geräte steigert aber andererseits auch die Attraktivität für die Mitarbeiter. Falls beispielsweise Gerätetypen über neuartige (biometrische) Authentifizierungs-Möglichkeiten oder neue Hardwareschnittstellen verfügen, so kann deren Wirksamkeit ohne entsprechendes Fachwissen nur eingeschränkt beurteilt werden.

6.2.7 Ungeregeltes Einspielen von Updates auf BYO-Geräten

Grundsätzlich ist es empfehlens- und wünschenswert ein BYO-Gerät auf dem aktuellen Softwarestand zu halten. Da das BYO-Gerät Eigentum des Mitarbeiters ist, hat er in der Regel auch umfangreiche Rechte auf diesem. Während auf institutseigenen Geräten die Administratoren entscheiden ob ein Softwareupdate installiert wird, so liegt dies auf einem BYO-Gerät standardmäßig in der Verantwortung des Mitarbeiters. Wenn der Mitarbeiter beispielsweise ein Update unmittelbar nach Erscheinen installiert, welches zu Inkompatibilitäten mit den institutionellen Anwendungen führt, kann dies zu einem Problem hinsichtlich der Verfügbarkeit führen. Vereinzelt sind Updates auch generell fehlerhaft und werden kurz nach dem Erscheinen wieder zurückgenommen. Eine IT-Administration wartet deshalb vor der Installation eines Updates in der Produktionsumgebung ggf. noch bzw. testet dieses vorab in einer Simulationsumgebung. Andererseits kann es jedoch auch problematisch sein, wenn der Mitarbeiter, etwa wegen der Inkompatibilität mit vorhandener Software, auf neue Updates verzichtet.

6.2.8 Automatisierte Synchronisation mit ungeeigneten Cloud-Diensten

Die umfangreicheren Rechte, die ein BYOD-Mitarbeiter auf seinem Gerät hat, geben ihm auch die Möglichkeit, Informationen mit externen Cloud-Diensten zu synchronisieren. Standardmäßig besteht dabei die Gefahr, dass dies auch institutionelle Informationen betreffen könnte und die Institution die Kontrolle darüber verliert, wo ihre Informationen gespeichert werden.

6.2.9 Ungeregelte Aussonderung von BYO-Geräten

Eine ungeregelte Aussonderung eines BYO-Geräts, bei dem etwa durch einen Defekt keine Löschung (Corporate-Wipe) mehr möglich war, stellt gegebenenfalls eine Gefahr für noch auf dem Gerät gespeicherte institutionelle Informationen dar.

6.2.10 Nicht oder unzureichend an BYOD angepasster Support

Die Möglichkeit zum zeit- und ortsunabhängigen Arbeiten mit BYOD stellt neue Herausforderungen an den Support der Institution. Es reicht ggf. nicht mehr aus einen Helpdesk während der Arbeitszeiten anzubieten, da BYOD-Mitarbeiter unter Umständen auch zu anderen Zeiten ein akutes Problem haben können, welches bei falscher Handhabung auch institutionelle Informationen gefährden kann.

6.2.11 Nutzung von BYO-Geräten durch Dritte

Haben Familienangehörige oder Freunde Zugang zum BYO-Gerät, können durch unsachgemäße Benutzung des Gerätes die institutionellen Informationen gefährdet werden.

6.3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.8 *BYOD* aufgeführt. Grundsätzlich ist der Bausteinverantwortliche für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und regelmäßig

überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)
Weitere Verantwortliche	Administrator, Benutzer, Datenschutzbeauftragter, Institutionsleitung, IT-Betrieb, Leiter IT, Leiter Organisation, Personalabteilung, Personalrat/Betriebsrat, Vorgesetzte

6.3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein CON.8 *BYOD* vorrangig umgesetzt werden:

CON.8.A1 Konzept für BYOD [Institutionsleitung, Leiter IT, Leiter Organisation, Vorgesetzte]

Gemäß dem Risikoappetit der Institution MUSS diese im Vorfeld festlegen, in welcher Form der Einsatz von BYOD für die Institution sinnvoll und akzeptabel ist. Dazu MÜSSEN die betroffenen Geschäftsprozesse, Programme und Daten der Institution analysiert und daraufhin bewertet werden, ob diese für BYOD zur Verfügung stehen sollten. Der tatsächliche Bedarf sowie die entstehenden Kosten MÜSSEN dabei ergänzend in Betracht gezogen werden. Zusätzlich MUSS sichergestellt werden, dass die benötigten Ressourcen in personeller und technischer Hinsicht vorhanden sind bzw. hergestellt werden. Weiter MUSS bereits an dieser Stelle die Strategie bzgl. der unterstützten Endgeräte und ggf. deren Einschränkungen festgelegt werden.

CON.8.A2 Regelungen für BYOD [Datenschutzbeauftragter, Institutionsleitung, Personalabteilung, Personalrat/Betriebsrat]

Die Institution MUSS ihren Mitarbeitern vorschreiben, wie BYOD stattfinden darf. Die Vereinbarung MUSS in Form einer Benutzerrichtlinie vor Freischaltung eindeutig akzeptiert werden. Mindestens muss darin geregelt werden:

- wer BYOD nutzen kann
- welche Voraussetzungen das Endgerät erfüllen muss

- das der Einsatz modifizierter Software grundsätzlich zu unterlassen ist
- in welchem Umfang BYOD eingesetzt werden kann
- unter welchen Bedingungen schützenswerte Informationen verarbeitet werden dürfen
- in welchem Umfang die Institution Zugriff auf das Gerät benötigt
- wie die privaten Informationen des Nutzers geschützt werden
- wie im Falle von Problemen Support geleistet wird
- welche Maßnahmen bei Verlust oder Diebstahl vorzunehmen sind
- wie sich die Nutzung von BYOD auf die Arbeitszeit auswirkt

CON.8.A3 Absicherung des Gerätes vor fremdem Zugriff [Benutzer]

Zur Absicherung des Gerätes MUSS ein Zugriffscode, -passwort oder eine vergleichbare Absicherung (Fingerabdruck, Gesichtsscanner etc.) gesetzt und aktiviert werden. Die Passwörter MÜSSEN der Passwort-Richtlinie der Institution entsprechen, siehe ORP.4 *Identitäts- und Berechtigungsmanagement*.

CON.8.A4 Nutzung einer abgesicherten Kommunikationsverbindung zur Institution [Benutzer]

Die Nutzung der Datendienste zur Institution MUSS über eine abgesicherte Kommunikationsverbindung nach Stand der Technik erfolgen.

CON.8.A5 Bereitstellung einer Liste unterstützter Plattformen und Softwareversionen [IT-Betrieb]

Damit Mitarbeiter sicher sein können, passende Geräte für BYOD anzuschaffen, MUSS eine verbindliche Aufstellung kompatibler Plattformen und (Mindest-) Softwareversionen zur Verfügung gestellt und regelmäßig aktualisiert werden.

6.3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein CON.8 *BYOD*. Sie SOLLTEN grundsätzlich umgesetzt werden.

CON.8.A6 Nutzung einer Software zum Gerätemanagement [Leiter IT, IT-Betrieb]

Zur besseren zentralisierten Verwaltung SOLLTE eine Software zum Gerätemanagement (MDM) eingesetzt werden. Werden institutionelle Informationen auf dem Gerät verarbeitet, SOLLTE zudem zur Trennung von den privaten Aktivitäten der Einsatz einer Management-Software mit Container-Lösung (MAM, EMM, UEM) geprüft werden. Die Auswahl der passenden Lösung SOLLTE anhand des geplanten Funktionsumfanges erfolgen.

CON.8.A7 Aktivierung automatischer Updates [Benutzer]

Damit immer die aktuellste Version des Betriebssystem genutzt wird, SOLLTE auf dem Endgerät die automatische Installation von Updates aktiviert und die Installation zeitnah vorgenommen werden.

CON.8.A8 Schulungen für BYOD [Personalabteilung, Vorgesetzte]

Um die Mitarbeiter für die BYOD-Nutzung und die damit verbundenen Gefährdungen zu sensibilisieren, SOLLTEN in Regelmäßigkeit Schulungen zu den relevanten Themen (Awareness) freiwillig oder verpflichtend angeboten werden.

CON.8.A9 Einschränkung der Nutzung von Software [Leiter IT, IT-Betrieb, Personalrat/Betriebsrat]

Zum Schutz der institutionellen Informationen vor ungeeigneter Verarbeitung SOLLTE der Einsatz einer Ausschluss- bzw. Freigabeliste (Black-/Whitelist) für Software geprüft werden. Diese SOLLTE als Bestandteil der Benutzerrichtlinie realisiert werden.

CON.8.A10 Aktivierung von Funktionen zur entfernten Verwaltung [Benutzer]

Zur Absicherung gegen Verlust und Diebstahl SOLLTEN Funktionen zur Sperrung und Löschung aus der Ferne aktiviert werden. Falls diese nicht über Gerätedienste zur Verfügung stehen, SOLLTEN entsprechende Zusatzdienste dafür genutzt werden. Zur Vereinfachung der Verwaltung SOLLTE auf eine Möglichkeit zur zentralen Verwaltung geachtet werden.

CON.8.A11 Aktivierung von Funktionen zur Absicherung [Benutzer]

Der Mitarbeiter SOLLTE verpflichtet werden, gerätespezifisch Hilfsprogramme wie ein Antivirus-Programm und eine Firewall zu installieren und auf dem aktuellen Stand zu halten. Zusätzlich SOLLTE ein sicherer Systemstart etwa durch Aktivierung des UEFI-SecureBoot (auf Notebooks) sichergestellt werden.

CON.8.A12 Aktivierung von Funktionen zur Verschlüsselung [Benutzer]

Um die auf dem Gerät lokal gespeicherten Daten bestmöglich zu schützen, SOLLTEN Dienste zur Echtzeit-Verschlüsselung der Daten (BitLocker, FileVault etc.) aktiviert werden. Die Auswahl SOLLTE unter Berücksichtigung von CON.1 *Kryptokonzept* erfolgen.

CON.8.A13 Anpassung des Supports für BYOD-Nutzung [Leiter IT, IT-Betrieb]

BYOD-Mitarbeiter SOLLTEN eine Unterstützung bei der Umsetzung der Anforderungen und auftretenden Problemen erhalten. Dieses Vorhaben kann mit der Bereitstellung von Informationen zur Selbsthilfe für häufig gestellte Fragen (FAQ) und Problemen, die außerhalb der Arbeitszeiten auftreten, realisiert werden. Hierfür SOLLTE geprüft werden, ob ergänzend eine Aufnahme in den üblichen Support der Institution vorgenommen werden kann.

CON.8.A14 Bereitstellung eines Teilnetzes innerhalb der Institution für BYOD [Leiter IT, IT-Betrieb]

Damit BYO-Geräte nur Zugriff auf die vorgesehenen Ressourcen erhalten, SOLLTE im Netzwerk der Institution explizit ein Teilnetz für diese Geräte eingerichtet werden.

6.3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein CON.8 *BYOD* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.8.A15 Steuerung von Software-Aktualisierungen [Leiter IT, IT-Betrieb] (C,I)

Zur Vermeidung von Inkompatibilitäten SOLLTE die Administration darüber entscheiden wann Software-Aktualisierungen aufgespielt werden.

CON.8.A16 Nutzung eindeutiger Identifizierung zum Zugriffsschutz [Leiter IT, IT-Betrieb] (C,I)

Zur Verbesserung der Sicherheit SOLLTE eine eindeutige Identifizierung und Freigabe von Diensten, etwa durch Zuhilfenahme der MAC-Adresse oder durch Nutzung von Fingerprinting des BYO-Geräts erfolgen.

CON.8.17 Nutzung von Zwei-Faktor-Authentifizierung [Benutzer] (C,I)

Zur Verbesserung der Sicherheit für schützenswerte Vorgänge SOLLTE, zusätzlich zum Zugriffscode, eine Zwei-Faktor-Authentifizierung eingesetzt werden.

6.4 Weiterführende Informationen

6.4.1 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein CON.8 *BYOD* finden sich unter anderem in folgenden Veröffentlichungen:

- Überblickspapier IT-Consumerisation und BYOD, BSI, Juli 2013, `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf?__blob=publicationFile&v=1`, zuletzt abgerufen am 28.04.2019

6.5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein CON.8 *BYOD* von Bedeutung.

- G 0.14 Ausspähen von Informationen/Spionage
- G 0.15 Abhören
- G 0.16 Diebstahl von Geräten, Datenträgern und Dokumenten
- G 0.17 Verlust von Geräten, Datenträgern und Dokumenten
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard und Software
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.36 Identitätsdiebstahl
- G 0.37 Abstreiten von Handlungen
- G 0.38 Missbrauch personenbezogener Daten
- G 0.42 Social Engineering
- G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

Die Kreuzreferenztabelle finden Sie aufgrund ihres Umfangs im Anhang A.2

7 Implementierung des IT-Grundschutz Bausteins

Dieses Kapitel untersucht eine erfolgreiche Implementierung von BYOD und dient der Erprobung der Praxistauglichkeit des Bausteins sowie einer weiteren Optimierung auf Basis dieser Erfahrungen. Dies kann jedoch aufgrund der Eigenschaften des IT-Grundschutzes nur in rudimentärer Weise erfolgen, da sich ein Baustein alleine nicht implementieren lässt, sondern nur als Bestandteil eines ISMS (Managementsystem für Informationssicherheit).

7.1 Erfolgsfaktoren

Zur Identifizierung von Schlüsselfaktoren für eine erfolgreiche Implementierung von BYOD, haben Yin et al. in ihrer Untersuchung ein Framework entwickelt [vgl. 50, S.5]:
Ausgehend von einem allgemein gültigen Modell mit der Bezeichnung „Gift Economy“ basiert die Annahme darauf, dass ein Gönner nach Unterstützung eines Empfängers auch immer eine Gegenleistung erwartet, damit er bereit ist, seine Unterstützung fortzusetzen. Auf BYOD angewendet formulieren Yin et al. es so, „that BYOD is a gift for employees when companies implement it because companies expect to be beneficial by their employees from BYOD implementation.“[50, S.4]
Weiter nutzen Yin et al. als zusätzliches Werkzeug die sogenannte „Cognitive Evaluation Theory“. Diese basiert lediglich auf zwei Grundbedürfnissen: Kompetenz und Autonomie. BYOD wirkt in diesem Fall als Variable unter zwei Aspekten: Informativ und Kontrollierend. Der informative Aspekt verbessert beim Mitarbeiter nach Ansicht von Yin et al. die Wahrnehmung von Kompetenz und führt zu besseren Arbeitsergebnissen. Auf der anderen Seite wirkt der kontrollierende Aspekt restriktiv und beeinflusst das Autonomie-Bedürfnis des Mitarbeiters, was zu schlechteren Arbeitsergebnissen führt.[vgl. 50, S.5]
Zusammenfassend resümieren Yin et al. wie folgt:

> „We propose that BYOD is a gift entered into the gift exchange process. Both informational aspect (such as flexibility, convenience, autonomy,

> and so on) and controlling aspect (such as workload, invisible control, and so on) can be perceived by employees. After that both positive and negative individual-level outcomes regarding to different aspects will be returned back, for example, satisfaction and/or organization commitment in the positive side and stress and/or burnout in the negative side. These returns will eventually affect organizational performance positively or negatively."[50, S.5]

Diese eigentlich triviale Aussage von Yin et al. verdeutlicht nochmals auf verständliche Weise, dass BYOD zwar ein weitläufiges Feld mit vielen Faktoren ist, aber es für den Erfolg eines BYOD-Programms im Kern auf das richtige Gleichgewicht von Freiheit und Kontrolle ankommt und das ein nachhaltiges Gelingen ohne die Unterstützung des Mitarbeiters schwerlich realisierbar ist.

7.2 Veröffentlichungsworkflow

Der in Kapitel 6 entwickelte Entwurf des Bausteins soll den Prozess einer erfolgreichen Implementierung von BYOD bestmöglich unterstützen. Damit dieser von Vornherein eine gute Praxistauglichkeit aufweist, sieht das BSI zur Erstellung neuer Bausteine eine gestufte Vorgehensweise vor [vgl. 14]. Dazu werden, wie in Abbildung 7.1 dargestellt, drei Phasen durchlaufen:

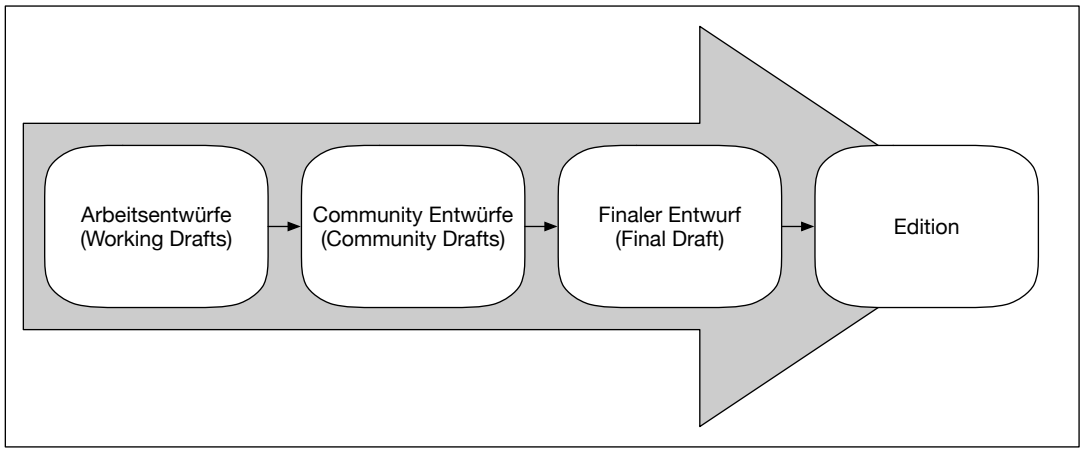

Abbildung 7.1: Veröffentlichungsworkflow des BSI für neue Bausteine

- **Working Draft:** Interner Arbeitsentwurf, der durch einen Autor mit Unterstützung eines BSI-Experten erarbeitet wurde. Es handelt sich um einen sehr groben Entwurf, der nur BSI-Intern verwendet wird.

- **Community Draft:** Veröffentlichung inklusive Umsetzungshinweisen zur Diskussion mit Anwendern und der Fachöffentlichkeit. Gegebenenfalls werden hier mehrere Versionen durchlaufen. Es wird überprüft, ob die Anforderungen verhältnismäßig und praxistauglich sind, ob Anforderungen oder Gefährdungen fehlen und ob noch Hinweise zur Umsetzung fehlen. Der Baustein hat an dieser Stelle bereits einen akzeptablen Reifegrad.
- **Final Draft:** Nach der Anpassung des Bausteins auf Basis der Rückmeldungen aus der Community, kann dieser im IT-Grundschutz-Kompendium veröffentlicht werden. Ein Final Draft an sich stellt bereits eine stabile Version mit Praxistauglichkeit dar. Da aufgrund von Zertifizierungsverfahren eine Aktualisierung der Edition nur einmal jährlich stattfindet, ist ein Final Draft eine Zwischenstufe um fertige Bausteine auch unterjährig veröffentlichen zu können und diese dann bei Überarbeitung der Edition mit einfließen zu lassen.

Der vorliegende Entwurf entspricht dem Arbeitsentwurf (Working Drafts) nach der ersten Phase. In dieser Form ist eine Praxistauglichkeit nicht garantiert und eine reale Implementierung noch nicht vorgesehen.

7.3 Validierung der Praxistauglichkeit

Auch wenn eine reale Implementierung im aktuellen Entwicklungsstand noch nicht möglich ist, so erscheint es zur Verbesserung und Optimierung des Entwurfs hilfreich, bereits teilweise die zweite Phase (Community Drafts) zu starten. Als „Community“ fungiert im Rahmen dieser Arbeit eine der Institutionen aus dem Bankensektor, die bei der Untersuchung zur aktuellen Umsetzung von BYOD in Kap. 2.4 bereits Auskunft gegeben hat.
Zur Befragung wurden der Institution Gefährdungen und Anforderungen aus einem Vorentwurf unter den folgenden Fragestellungen zur Verfügung gestellt.

- Sind die thematisierten Gefährdungen praxisrelevant und haben auch für das Institut Gültigkeit?
- Sind die formulierten Anforderungen angemessen und praxistauglich bzw. bereits realisiert?
- Gibt es noch Gefährdungen oder Anforderungen, die noch nicht berücksichtigt wurden?

Im Gespräch mit dem Informationssicherheitsbeauftragten der Institution wurde (für das dort eingesetzte Szenario) Feedback zum Vorentwurf gegeben. Folgende Notizen wurden dazu angefertigt:

- **Gefährdungen:** Grundsätzlich wurde allen genannten Gefährdungen hinsichtlich der Relevanz für BYOD zugestimmt. Details zur Einordnung wurden wie folgt genannt:
  - **Vermischung privater und beruflicher Daten:** Da auf klassischen BYO-Geräten der Institution nur eingeschränkter Zugriff ohne Informationstransfer stattfindet, ist dies in diesem Szenario nicht zutreffend. Auf dienstlichen Geräten mit erweiterten Funktionen wird die Datentrennung durch ein MDM sichergestellt. Die DSGVO greift ohnehin und Mitarbeiter sind selbstverantwortlich keine sensiblen institutionellen Informationen auf ihrem Gerät zu sichern.
  - **Unzureichende Administrationsmöglichkeiten für institutionellen Einsatz:** Administration wird mittels MDM geregelt. Durch Beschränkung auf iOS-basierte Geräte wird zudem die Vielfalt reduziert.
  - **Fehlende Rechtssicherheit im Umgang mit BYOD:** Absicherung über Nutzungsvereinbarung. Corporate-Wipe auch bei BYO-Geräten möglich.
  - **Fehlende Regelung zu Arbeitszeiten mit BYOD:** Der BYOD-Einsatz ist als Optional definiert und liegt in der Eigenverantwortung des Mitarbeiters. Dieser ist dienstlich angewiesen für seinen Arbeitsschutz selber Sorge zu tragen.
  - **Fehlende Softwarelizenzen für den BYOD-Einsatz:** Mittels Beschränkung der Dateibearbeitung auf Container-Apps auf dienstlichen Geräten wird das Problem in dieser Konstellation vermieden.
  - **Kurze Lebenszyklen mit heterogenen Geräten überfordern Administration:** Die explizite Beschränkung auf iOS-basierte Geräte grenzt die Menge der unterschiedlichen Gerätegenerationen deutlich ein.
  - **Ungeregeltes Einspielen von Updates auf BYO-Geräten gefährdet Verfügbarkeit:** Für dienstliche Geräte erfolgt ein Test und eine Freigabe neuer Software-Versionen. Es besteht keine Verpflichtung für automatische Aktualisierungen sondern nur eine Mindestversion als Voraussetzung. Eine Steuerung von Aktualisierungen mittels des MDM findet nicht statt.
  - **Automatisierte Synchronisation mit ungeeigneten Cloud-Diensten:** Softwareseitiger Ausschluss der Nutzung von Cloud-Diensten auf dienstlichen Geräten (mittels MDM) bzw. keine Möglichkeit zum Zugriff auf die Daten im Container. Bei privaten BYO-Geräten befinden sich keine relevanten Daten auf dem Gerät und werden somit auch nicht durch eine mögliche Synchronisierung tangiert.

  - **Ungeregelte Aussonderung von BYO-Geräten gefährdet institutionelle Informationen:** Da sensible Informationen lediglich auf dienstlichen Geräten vorliegen können und diese nicht durch den Mitarbeiter veräußert bzw. entsorgt werden dürfen, liegt die Verantwortung zur ordnungsgemäßen Aussonderung bei der Institution. Auf BYO-Geräten sind mit dem einseitigen Entzug des Zugangs auf Seiten der Institution keine Daten mehr abrufbar.

  - **Nicht oder unzureichend an BYOD angepasster Support der Institution gefährdet Abläufe:** Der Support steht nur während der Kernarbeitszeiten zur Verfügung. Überdies gibt es für BYOD keinen gesonderten Support, sondern Selbsthilferessourcen (individuelle Handbücher zur Benutzung) im Intranet. Dies hat sich als ausreichend für das gegebene Szenario herausgestellt.

  - **Nutzung von BYO-Geräten durch Dritte:** Mittels Arbeitsanweisung wird dem Benutzer untersagt Zugriff auf institutionelle Informationen für Dritte zu gestatten. Dies liegt in seiner Verantwortung und trifft auf BYO-Geräten genauso wie auch auf dienstliche Geräte zu.

- **Anforderungen:** Bezüglich der Anforderungen gab es grundsätzlich Zustimmung, aber auch Anregungen bestimmte Punkte zwischen Basis- und Standard-Anforderungen zu verschieben oder anders zu formulieren. Das Feedback im Detail:

  - **Absicherung des Geräts vor fremdem Zugriff:** Durch MDM-Nutzung sind sichere Passwörter (mit regelmäßiger Neubewertung) obligatorisch. Fingerabdruck-Authentifikation wird ebenfalls, sofern technisch verfügbar, mittels MDM verlangt.

  - **Online-Benutzerrichtlinien für BYOD:** Arbeitsanweisungen, die per Unterschrift zu bestätigen sind, regeln diese Punkte im Vorfeld.

  - **Nutzung einer abgesicherten Kommunikationsverbindung zur Institution:** Notwendig und durch Einsatz eines MDM obligatorisch.

  - **Bereitstellung einer Liste unterstützter Endgeräte:** Beschränkung auf iOS-basierte Geräte und damit verbunden lediglich eine Bereitstellung der notwendigen Mindestversion des Betriebssystems.

  - **Setzen von Anreizen durch Unterstützung aktueller Gerätegenerationen:** Aktuelle Gerätegenerationen sind grundsätzlich immer aufgrund der unterstützten Mindestversion des Betriebssystems kompatibel.

- **Schulungen für BYOD:** Werden lediglich für dienstliche iPads im Vertrieb vorgenommen, aber beziehen sich mehr auf den Umgang mit dem Gerät als auf spezielle BYOD-Funktionen. Eine spezielle Schulung wird in diesem Szenario ansonsten für nicht notwendig erachtet, da die betroffenen Mitarbeiter bereits Fertigkeiten mitbringen.

- **Aktivierung automatischer Updates:** Nutzung ist nicht verpflichtend, es wird vielmehr nur eine Mindestversion gefordert, die regelmäßig nachgezogen wird.

- **Aktivierung der Zwei-Faktor-Authentifizierung:** Wird nicht eingesetzt und nach Erfahrung nicht notwendig erachtet.

- **Aktivierung von Funktionen zur entfernten Verwaltung:** Da bei BYO-Geräten keine Daten gespeichert werden, erfolgt bei Verlust lediglich eine einseitige Maßnahme in Form der Sperrung des Accounts zum Institutionsnetzwerk. Bei dienstlichen Geräten ist ein Remote-Wipe möglich, jedoch keine Ortung. Dies wird als rechtlich fragwürdig eingestuft und zugleich nicht benötigt.

- **Aktivierung von Funktionen zur Absicherung:** Aufgrund der Beschränkung auf die iOS-Plattform im BYOD-Bereich, ist dies nur bei der Nutzung von Laptops etwa zum Remotezugang notwendig. Eine Dienstanweisung schreibt entsprechend die Nutzung eines Antiviren-Scanners vor.

- **Aktivierung von Funktionen zur Verschlüsselung:** Da lediglich iOS-basierte Geräte akzeptiert werden, ist die Dateiverschlüsselung standardmäßig aktiviert.

- **Nutzung einer Software zum Gerätemanagement:** Als MDM kommt MobileIron zum Einsatz und es wird empfohlen, die Notwendigkeit eines MDM aus organisatorischen und rechtlichen Gesichtspunkten in die Basis-Anforderungen zu verschieben.

- **Anpassung des Supports für BYOD-Nutzung:** Für einen erweiterten Support wird beim vorliegenden Szenario keine Notwendigkeit gesehen. Zudem wird empfohlen, die 24/7-Regelung aus den Standard-Anforderungen zu löschen.

- **Mitarbeiterzertifizierung für BYOD:** Eine Form der Zertifizierung zu BYOD wird, aus der Erfahrung heraus, nicht für notwendig gehalten.

- **Nutzung der MAC-Adresse zum Zugriffsschutz:** Eine Prüfung der MAC-Adresse zum Zugriffsschutz erfolgt lediglich bei physikalischer Verbindung im Unternehmensnetzwerk. Ansonsten erfolgt die Authentifizierung nur über Zertifikate.
- **Steuerung von Software-Aktualisierungen:** Via MDM zwar möglich, wird aber aufgrund des Ansatzes mit Mindestversionen nicht benötigt.

7.4 Konsolidierung und Optimierung

Die Simulation durch Befragung und die daraus gewonnenen Ergebnisse haben ergeben, dass dieser Entwurf grundsätzlich eine gute Basis für Institutionen, die ein BYOD-Programm einführen möchten, darstellen sollte. Die Vielfältigkeit der möglichen Szenarien machen es erwartungsgemäß notwendig, die Konstellationen auf gängige Muster zu beschränken. Das Feedback seitens der Institution bezieht sich auch lediglich auf das dort aktuell eingesetzte Szenario, hat aber trotzdem nützliche Informationen bereitgestellt. Folgende Modifikationen am Entwurf wurden aufgrund der Rückmeldung aus der Praxis in Erwägung gezogen:

- **Wechsel von der Notwendigkeit des Einsatzes aktueller Systemsoftware hin zu Mindestversionen:** Diese Änderung ist hinsichtlich der Basis-Anforderung eine sinnvolle Ergänzung um auch die Plattformen nach unten hin abzugrenzen.
- **Forderung nach automatischer Aktualisierung in den Bereich für erhöhten Schutzbedarf:** Nach Abgleich mit den Recherche-Ergebnissen ist eine aktuelle Software, als wesentliches Mittel zur Entfernung von Sicherheitslücken, eine sinnvolle Anforderung in den Standard-Anforderungen und bleibt deshalb an dieser Stelle.
- **Verschiebung der Forderung einer MDM-Lösung in die Basis- Anforderungen sowie Aufnahme der Empfehlung einer Container-Lösung (MAM) in den Standard-Anforderungen:** Mit Beachtung der rechtlichen Lage und der organisatorischen Situation scheint es tatsächlich zunächst sinnvoll zu sein, die Nutzung einer MDM-Lösung in die Basisanforderungen zu integrieren. Auch in der Recherche wurde festgestellt, dass ein MDM für BYOD sehr wichtig ist. Unter Berücksichtigung der Tatsache, dass der Baustein im IT-Grundschutz aber auch Szenarien mit weniger Komplexität unterstützen soll, wäre eine verbindliche Nutzung einer MDM-Lösung jedoch überzogen. Es wurde deshalb die Lösung favorisiert, eine gemeinsame Anforderung für MDM und MAM in den Standardanforderungen zu formulieren.

- **Verschiebung der Empfehlung für Schulungen in den Bereich für erhöhten Schutzbedarf:** Schulungen, gerade zu Awareness-Themen gehören zu den wichtigen Werkzeugen einer Institution um Gefährdungen durch falsches Verhalten des Mitarbeiters zu vermeiden. Aus diesem Grunde sind, auch wenn es im konkreten Fall aus der Praxis nicht für notwendig erachtet wird, Schulungen eine sinnvolle Anforderung in den Standard-Anforderungen. Die Einschätzung zur nicht notwendigen Forderung von Mitarbeiterzertifizierungen zu BYOD ist nachvollziehbar und die Anforderung wurde daraufhin entfernt.

Zusätzlich wurde in einer Kontrollrunde mit dem BSI noch eine Anforderung hinsichtlich eines "Konzepts für BYOD" integriert und weitere Optimierungen am Baustein durchgeführt.

Der „Working Draft" für den Baustein findet sich in Kap. 6 und gemäß der Formatierung des BSI als Datei auf dem beiliegenden Datenträger.

8 Schlussfolgerung

Zusammenfassend lässt sich festhalten, dass das Thema *Consumerisation und BYOD* im institutionalen Umfeld zunehmend benötigt und auch gefordert wird. Dadurch wird die Organisation einer Institution vor neue Herausforderungen im organisatorischen, technischen und rechtlichen Bereich gestellt. Dies erfordert ein strukturiertes Vorgehen mit einer Bedarfsanalyse, die auch die Mitarbeiter mit einbezieht, einer schrittweisen Einführung und einer nachhaltigen Strategie hinsichtlich Sicherheit und Leistung des BYOD-Programms.

Gerade die gemeinsame Verwaltung von privaten und institutionellen Informationen auf einem Gerät und die damit verbundenen datenschutzrechtlichen Aspekte stellen neue Anforderungen und erfordern spezielle (sicherheitstechnische) Maßnahmen. Dies lässt sich (je nach Funktionsumfang) mit herkömmlichen Techniken nicht erreichen, weshalb spezielle Software, so genannte Management-Lösungen, zum Einsatz kommen müssen. Die Hersteller der verbreiteten Betriebssysteme haben dafür bereits Schnittstellen in ihren Distributionen vorgesehen.

Für eine hohe Attraktivität des BYOD-Programms sollten möglichst viele unterschiedliche Gerätetypen in den Informationsverbund integrierbar sein. Die Funktionsweisen und Betriebssysteme von Gerätetypen wie Smartphones und Tablets benötigen hierzu spezielle Kompetenzen in der IT-Abteilung.

Mit Interesse an den derzeit praktizierten BYOD-Strategien wurden einige Institutionen kontaktiert und um Mithilfe gebeten. Die Möglichkeiten, Auskunft hinsichtlich dieser sicherheitsrelevanten Themen zu geben, waren erwartungsgemäß beschränkt. Trotzdem gab es bei den beteiligten Unternehmen Bemühungen einen Überblick zu ihrer aktuellen Umsetzung zu geben. An dieser Stelle nochmals vielen Dank für die Unterstützung! In dieser kleinen Stichprobe wurde deutlich, dass die Strategien recht vergleichbar sind. Auffällig in diesem Zusammenhang ist vor allem, dass Unternehmen aktuell hinsichtlich der Unterstützung smarter Geräte eher die restriktivere iOS-basierte Schiene unterstützen und die Android-basierten Geräte bei größerem Funktionsumfang eher außen vor bleiben. Weiter haben die Schwierigkeiten über Auskunft zum aktuellen Stand auch gezeigt, dass sich die Unternehmen hinsichtlich BYOD in einem fortwährenden Prozess befinden, der regelmäßig erweitert wird.

Der *IT-Grundschutz* des BSI hatte bisher keinen dezidierten Baustein zur Berücksichtigung der BYOD-Thematik. Aus diesem Grunde wurde im Rahmen einer Risikoanalyse nach dem Vorgehen des BSI ein Baustein konzipiert und bis zum Arbeitsentwurf entwickelt. Die Ergebnisse wurden mit Unterstützung der befragten Institution hinsichtlich ihrer Relevanz und Praxistauglichkeit bewertet und dadurch bereits erste Hinweise für mögliche Optimierungen gewonnen. Gemäß dem *Veröffentlichungsworkflow* des BSI wird dieser Stand nun die Phasen bis zum finalen Entwurf weiter durchlaufen und dann in das IT-Grundschutz-Kompendium überführt.

Auch wenn BYOD aktuell tendenziell positiv bewertet wird, wird sich in Zukunft zeigen, ob sich dieser Trend so fortsetzen lässt. Das Streben nach „Entschleunigung“ steht im Konflikt zur theoretischen Möglichkeit der „24/7“-Erreichbarkeit mittels BYOD. Ein weiteres, schwieriges Kriterium ist die rechtliche Seite hinsichtlich des Datenschutzes aber auch der Arbeitszeitregelung. Diese Fragestellungen machen bereits heute eine umfassende Planung unentbehrlich.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] Apple. iOS Security. *apple.com*, 2018. [https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf; abgerufen am 23.03.2019].

[2] Apple. macOS Security - Overview for IT. *apple.com*, 2018. [https://www.apple.com/business/resources/docs/macOS_Security_Overview.pdf; abgerufen am 12.03.2019].

[3] Apple. Apple T2 Security Chip - Security Overview. *apple.com*, 2018. [https://www.apple.com/mac/docs/Apple_T2_Security_Chip_Overview.pdf; abgerufen am 28.01.2019].

[4] Dominique Assing und S. Cale. *Mobile Access Safety, Beyond BYOD*. ISTE Ltd, London, 2013. ISBN 978-1-84821-435-4.

[5] BITKOM. Arbeit 3.0 - Arbeiten in der digitalen Welt. *bitkom.de*, 2015. [https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2013/Studien/Studie-Arbeit-3-0/Studie-Arbeit-30.pdf; abgerufen am 26.01.2019].

[6] Mathias Brandt. Tablets: The Hype is Over. *statista.com*, 2014. [https://www.statista.com/chart/2829/worldwide-mobile-device-sales-forecast/; abgerufen am 11.04.2019].

[7] Manfred Bremmer. Mit UEM werden die Karten neu gemischt. *computerwoche.de*, 2018. [https://www.computerwoche.de/a/mit-uem-werden-die-karten-neu-gemischt,3545573; abgerufen am 23.02.2019].

[8] Christina Bröhl, P. Rasche, J. Jablonski, S. Theis, M. Wille, und A. Mertens. Desktop PC, Tablet PC, or Smartphone? An Analysis of Use Preferences in Daily Activities for Different Technology Generations of a Worldwide Sample. 2018.

[9] BSI, Bonn. BSI-Standard 200-1: Managementsysteme für Informationssicherheit, 2017. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.pdf?__blob=publicationFile&v=6].

[10] BSI, Bonn. BSI-Standard 200-2: IT-Grundschutz-Methodik, 2017. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=6].

[11] BSI, Bonn. BSI-Standard 200-3: Risikomanagement, 2017. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3].

[12] BSI, Bonn. BSI SYS.1.6 Container - Community Draft, 2018. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Container.pdf?__blob=publicationFile&v=4].

[13] BSI, Bonn. BSI-Kompendium 1. Edition 2018, 2018. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2018.pdf?__blob=publicationFile&v=7].

[14] BSI, Bonn. Erstellung von Bausteinen: Veröffentlichungsworkflow. *bsi.de*, 2018. [https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GS_Drafts/Workflow/wf_drafts_node.html; abgerufen am 10.11.2018].

[15] Randall Cameron. MDM to EMM to UEM – a Mobile Journey. *mobile-mentor.com*, 2018. [https://www.mobile-mentor.com/blog/unified-endpoint-management-2018; abgerufen am 23.02.2019].

[16] Marika de Bruijne und A. Wijnant. Comparing Survey Results Obtained via Mobile Devices and Computers: An Experiment With a Mobile Web Survey on a Heterogeneous Group of Mobile Devices Versus a Computer-Assisted Web Survey. *Social Science Computer Review*, (31(4)), 2013. [https://journals.sagepub.com/doi/10.1177/0894439313483976; abgerufen am 15.01.2019].

[17] Wilhelm Dolle und C. Wegener. Trusted Computing für Linux: Stand der Dinge. *linux-magazin.de*, 2006. [http://www.linux-magazin.de/ausgaben/2006/04/hoellenglut/; abgerufen am 11.03.2019].

[18] Dynamic Markets. Tablets and the european productivity revolution. *business.panasonic.de*, 2018. [https://business.panasonic.de/computerloesungen/sites/default/eu-files/news_files/DYNAMIC_MARKETS_Whitepaper_Tablets_and_the_European_Productivity%20Revolution.pdf; abgerufen am 03.01.2019].

[19] Moritz Förster. MDM, MAM oder EMM? Smartphones in Unternehmen verwalten. *iX - Magazin für professionelle Informationstechnik*, 2017. [https://www.heise.de/ix/meldung/MDM-MAM-oder-EMM-Smartphones-im-Unternehmen-verwalten-3796434.html; abgerufen am 17.01.2019].

[20] Dr. Andreas Gentner. Immer und überall: Smartphone bestimmt unseren Alltag. *Deloitte.*, 2018. [https://www2.deloitte.com/de/de/pages/presse/contents/studie-2018-im-Smartphone-Rausch.html; abgerufen am 23.12.2018].

[21] Sebastian Günther und M. Zimmermann. Fest verschlossen. *iX - Magazin für professionelle Informationstechnik*, (07):116–119, 2018.

[22] Bob Hayes und K. Kotwica. *Bring Your Own Device (BYOD) to Work, Trend Report*. The Security Executive Council. Published by Elsevier Inc., Waltham, MA 02451, USA, 2013. ISBN 978-0-12-411592-7.

[23] Heise. SSDs in der Praxis nicht zuverlässiger als Festplatten. *heise.de*, 2015. [https://www.heise.de/newsticker/meldung/SSDs-in-der-Praxis-nicht-zuverlaessiger-als-Festplatten-2560979.html; abgerufen am 28.02.2019].

[24] Chris Hoffman. How to Make BitLocker Use 256-bit AES Encryption Instead of 128-bit AES. *howtogeek.com*, 2014. [https://www.howtogeek.com/193649/how-to-make-bitlocker-use-256-bit-aes-encryption-instead-of-128-bit-aes/; abgerufen am 12.03.2019].

[25] Anat Hovav und F. Ferdani Putri. This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, (32):35–49, 2016. [https://doi.org/10.1016/j.pmcj.2016.06.007; abgerufen am 20.12.2018].

[26] ISO/IEC. Template for comments and secretariat observations. *netzpolitik.org*, 2014. [https://cdn.netzpolitik.org/wp-upload/ISO_IEC_11889-4_DIN.pdf; abgerufen am 12.03.2019].

[27] Andreas Kohne, S. Ringleb, und C. Yücel. *Bring your own Device - Einsatz von privaten Endgeräten im beruflichen Umfeld - Chancen, Risiken und Möglichkeiten.* Springer Vieweg, Wiesbaden, 2015. ISBN 978-3-658-03717-8.

[28] Bernd Kretschmer. Schlankheitskur. *iX - Magazin für professionelle Informationstechnik*, (03), 2007.

[29] Cornelius Kölbel. Vervielfacht - Authentifizierungsverfahren für Unternehmen. *iX - Magazin für professionelle Informationstechnik*, (07), 2016.

[30] Peter Lugtig und V. Toepoel. The Use of PCs, Smartphones, and Tablets in a Probability-Based Panel Survey: Effects on Survey Measurement Error. *Social Science Computer Review*, (31(1)), 2015. [https://journals.sagepub.com/doi/10.1177/0894439315574248; abgerufen am 15.01.2019].

[31] Marte Dybevik Løge. Tell me who you are and I will tell you your unlock pattern. *NTNU*, 2015. [http://masui.org.s3.amazonaws.com/b/7/b7591b5f8b6edd3f7d54372b6c3ad496.pdf; abgerufen am 21.03.2019].

[32] David MacQueen. Augmented Reality is Taking Off, but Dedicated AR Headsets Remain Grounded. *strategyanalytics.com*, 2018. [https://news.strategyanalytics.com/press-release/ux-innovation/strategy-analytics-augmented-reality-taking-dedicated-ar-headsets; abgerufen am 28.12.2018].

[33] Jens Mahnke und R. Frankenstein. Report: Durchleuchtet - Analyse TLS-verschlüsselter Netzwerkkommunikation. *iX - Magazin für professionelle Informationstechnik*, (02):96, 2019.

[34] MobileIron. Der ultimative Leitfaden zu BYOD. *mobileiron.com*, 2018. [https://www.mobileiron.com/de/resources-library/whitepapers/ultimate-guide-byod; abgerufen am 15.12.2018].

[35] Christine Monsch. *BYOD, Rechtsfragen der dienstlichen Nutzung arbeitnehmereigener mobiler Endgeräte im Unternehmen*. Duncker und Humblot, Berlin, 2017. ISBN 978-3-428-55016-6. Schriften zum Sozial- und Arbeitsrecht, Band 344.

[36] NIST. BitLocker Drive Encryption Security Policy. *nist.gov*, 2011. [https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp1054.pdf; abgerufen am 12.03.2019].

[37] Prof. Dr.-Ing. Christof Paar und Dr. J. Pelzl. *Understanding Cryptographie*. Springer, Bochum, 2010. ISBN 978-3-642-041000-6.

[38] Prey. Mobile Theft & Loss Report. *preyproject.com*, 2019. [https://preyproject.com/blog/wp-content/uploads/2019/02/Mobile-Theft-Loss-Report-2018.pdf; abgerufen am 07.03.2019].

[39] Christoph Puppe. Report: Trendiger Schutz - Entwurf des BSI-Bausteins zu Containern. *iX - Magazin für professionelle Informationstechnik*, (07):108–110, 2018.

[40] Michael H. Quade und U. Leimstoll. Mobile Business with Smartphones and Tablets: Effects of Mobile Devices in SMEs. *BLED 2015 Proceedings*, (12), 2015. [http://aisel.aisnet.org/bled2015/12; abgerufen am 10.04.2019].

[41] Lukas Scherenschleifer. Packungsbeilage TPM. *netzpolitik.org*, 2016. [https://trustedwindows.wordpress.com/2016/06/07/packungsbeilage-tpm/; abgerufen am 12.03.2019].

[42] Uwe Schulze. Mobile Firmenzugänge: VPN und die Alternativen. *iX - Magazin für professionelle Informationstechnik*, (05), 2011.

[43] Jörg Schwenk. *Sicherheit und Kryptographie im Internet*. Springer Vieweg, Bochum, 2014. ISBN 978-3-658-06543-0.

[44] Absolute Software. Germany mobile enterprise risk survey. *Absolute Software*, 2013. [`http://www.absolute.com/en/resources/research/mobile-enterprise-risk-germany`; abgerufen am 11.12.2018].

[45] Bruce Taplin. *Smartphone History: Evolution and Revolution*. Amazon Media, 2013.

[46] Kevin Timms. BYOD must be met with a wider appreciation of the cybersecurity threat. *Computer Fraud and Security*, (7):5–8, 2017.

[47] Brian Tokuyoshi. The security implications of BYOD. *Network Security*, (4): 12–13, 2013.

[48] U. Vignesh und S. Asha. Modifying security policies towards BYOD. *Procedia Computer Science*, (50).

[49] Thorsten Walter. *Bring your own Device - Ein Praxisratgeber*. Springer Vieweg, Wiesbaden, 2015. ISBN 978-3-658-11591-3. HMD Best Paper Award 2014.

[50] ChunXiao Yin, L. Liu, und L. Liu:. Byod Implementation: Understanding Organizational Performance through a Gift Perspective. *PACIS*, (129).

[51] Nima Zahadat, P.Blessner, T. Blackburn, und B. A. Olson. BYOD security engineering: A framework and its analysis. *ScienceDirect*, (55):81–99, 2015.

A Anhang

Gartner Magic Quadrant UEM

Abbildung A.1: Quelle: [7]

Tabelle A.2: Kreuzreferenztabelle

CON.8	G0.14	G0.15	G0.16	G0.17	G0.18	G0.19	G0.20	G0.21	G0.26	G0.27	G0.36	G0.37	G0.38	G0.42	G0.47
CON.8.A1	X	X			X	X				X			X		X
CON.8.A2	X	X	X	X	X	X	X				X	X	X		
CON.8.A3	X		X	X							X	X	X		X
CON.8.A4	X	X				X									X
CON.8.A5					X		X			X					X
CON.8.A6	X	X	X	X	X	X	X	X	X	X			X		
CON.8.A7					X		X		X						X
CON.8.A8	X	X	X	X	X	X	X	X	X		X		X	X	
CON.8.A9		X			X		X		X	X			X		X
CON.8.A10			X	X		X									
CON.8.A11	X	X				X	X	X	X						X
CON.8.A12	X		X	X		X									X
CON.8.A13					X			X	X	X				X	
CON.8.A14	X	X				X	X	X			X				X
CON.8.A15					X		X		X						X
CON.8.A16						X					X	X		X	
CON.8.A17	X	X	X	X		X					X	X		X	

Benutzerdefinierter Baustein

CON: Konzeption und Vorgehensweise

CON.bd.8: BYOD

1 Beschreibung

1.1 Einleitung

Mobilität und Flexibilität sind, auch bei der IT-Nutzung einer Institution, selbstverständlich geworden. Die Anforderung, unterwegs sicher seine E-Mails oder Termine abzurufen oder auf das Institutionsnetzwerk zugreifen zu können, ist technisch möglich. Zunehmend gewünscht wird in diesem Zusammenhang die kombinierte Nutzung eines IT-Gerätes für berufliche und private Zwecke, wodurch neue Herausforderungen für die Informationssicherheit entstehen. Private und institutionelle Informationen müssen auseinander gehalten sowie unterschiedliche Hardware in den Informationsverbund integriert und verwaltet werden.

Je nach Ausprägung wird in diesem Zusammenhang von Consumerisation oder Bring your own Device (BYOD) gesprochen. Während Consumerisation als Teilmenge von BYOD lediglich die private Nutzung institutionseigener Geräte umfasst, so steht BYOD für den Einsatz von selbstständig angeschafften (ggf. subventionierten) Geräten der Mitarbeiter im privaten und beruflichen Bereich.

Die Anforderungen an die Institution hinsichtlich der Umsetzung sind vielfältig auf organisatorischer, Applikations- und Geräteebene angesiedelt.

1.2 Zielsetzung

Ziel des Bausteins ist die Integration von mitarbeitereigenen Geräten, die nicht im Einfluss des Arbeitgebers stehen. Dazu werden typische Gefährdungen aufgezeigt und spezielle Anforderungen an BYOD gestellt.

1.3 Abgrenzung

Dieser Baustein konzentriert sich auf die sicherheitstechnischen Besonderheiten, mit denen Institutionen durch die Einführung von BYOD konfrontiert werden. BYOD als Nutzungskonzept erstreckt sich über verschiedene Bereiche mit organisatorischen, technischen und rechtlichen Aspekten. Dadurch sind auch vermehrt Kontaktpunkte mit anderen Bausteinen gegeben, die bei der Umsetzung zu beachten sind.

Sicherheitsanforderungen an die Endgeräte und deren Betriebssysteme werden im vorliegenden Baustein nicht berücksichtigt, sondern sind Bestandteil der jeweiligen Bausteine unter SYS: *IT-Systeme*.

Es wird ferner eine funktionierende Kommunikationsverbindung vorausgesetzt, welche entweder über eine Datenverbindung eines Telekommunikationsdienstleisters hergestellt oder mittels einer WLAN-Verbindung (NET.2.2: *WLAN-Nutzung*) realisiert wird. Zur Absicherung der Verbindung wird zusätzlich auf den Baustein NET.3.3: *VPN* verwiesen.

Organisatorische Grundlagen liefern die Bausteine aus ORP: *Organisation und Personal*.

Die Anforderungen aus dem themenüberschneidenden Baustein SYS.3.2.2 *Mobile Device Management (MDM)* und OPS.1.2.4 *Fernwartung* sind zu beachten.

Weitere, auch für BYOD gültige Aspekte, finden sich in:

- INF.8 *Häuslicher Arbeitsplatz*
- INF.9 *Mobiler Arbeitsplatz*
- OPS.1.2.4 *Telearbeit*
- CON.7 *Informationssicherheit auf Auslandsreisen*

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein CON.bd.8 *BYOD* von besonderer Bedeutung:

2.1 Vermischung privater und beruflicher Informationen

Wenn auf einem Gerät sowohl private als auch berufliche Informationen gespeichert werden, besteht die Gefahr, dass diese Informationen nicht ausreichend voneinander getrennt sind. Dies geschieht beispielsweise durch Programme, die vollständigen Zugriff auf das Adressbuch anfordern. Sollten hier auch institutionelle Informationen betroffen sein, hat dies datenschutzrechtliche Relevanz.

2.2 Unzureichende Administrationsmöglichkeiten für institutionellen Einsatz

Mobile Endgeräte sind im Hinblick auf die Konfigurationsmöglichkeiten zumeist für den Consumer-Bereich vorgesehen und bieten von Hause aus keine erweiterten Optionen wie sie im Unternehmensbereich benötigt werden. Ein einfaches Beispiel ist der explizite Nutzungsausschluss von Systemapplikationen wie Bildschirmfotos.

2.3 Fehlende Rechtssicherheit im Umgang mit BYOD

Wenn mit BYOD neu auftretende Rechtsfragen nicht ausreichend geregelt sind, kann es im späteren Betrieb zu Irritationen über Rechte und Pflichten kommen. Dies gilt zum Beispiel für die Frage, ob die Institution das Recht hat, das Gerät im Falle eines Verlusts aus der Ferne zu löschen.

2.4 Fehlende Regelung zu Arbeitszeiten mit BYOD

Durch BYOD gewinnt der Arbeitnehmer zwar an Flexibilität hinsichtlich seiner Arbeitszeit, gleichzeitig birgt jedoch die ständige Erreichbarkeit auch Gefahren. Die Institution verliert ihrerseits Kontrolle darüber, wann der Mitarbeiter arbeitet und wann nicht. Mit Berücksichtigung der möglichen Anrechnung als Arbeitszeit, sobald die Institution eine Bereitschaft aktiv einfordert, sollten bereits im Vorfeld entsprechende Regelungen stattfinden.

2.5 Fehlende Softwarelizenzen für den BYOD-Einsatz

Wird institutionelle Software auf dem privaten Endgerät genutzt, so besteht die Möglichkeit, dass Software eingesetzt wird, die in diesem Kontext lizenzrechtlich nicht ausreichend abgesichert ist. In gleicher Weise gilt dies auch für privat erworbene Software/Apps, die durch den Arbeitnehmer für dienstliche Zwecke genutzt werden könnte. Dies kann für den Mitarbeiter als auch die Institution rechtliche Schwierigkeiten und damit verbundene Kosten nach sich ziehen.

2.6 Fehlende Anpassung an neue Gerätegenerationen

Der mögliche Wunsch der Arbeitnehmer nach Nutzung aktueller Gerätegenerationen, birgt die Gefahr, dass der IT-Betrieb nicht über das notwendige Fachwissen verfügt und eine sichere Integration nicht in jedem Fall

gewährleisten kann. Die Unterstützung aktueller Geräte steigert aber andererseits auch die Attraktivität für die Mitarbeiter. Falls beispielsweise Gerätetypen über neuartige (biometrische) Authentifizierungs-Möglichkeiten oder neue Hardwareschnittstellen verfügen, so kann deren Wirksamkeit ohne entsprechendes Fachwissen nur eingeschränkt beurteilt werden.

2.7 Ungeregeltes Einspielen von Updates auf BYO-Geräten

Grundsätzlich ist es empfehlens- und wünschenswert ein BYO-Gerät auf dem aktuellen Softwarestand zu halten. Da das BYO-Gerät Eigentum des Mitarbeiters ist, hat er in der Regel auch umfangreiche Rechte auf diesem. Während auf institutseigenen Geräten die Administratoren entscheiden ob ein Softwareupdate installiert wird, so liegt dies auf einem BYO-Gerät standardmäßig in der Verantwortung des Mitarbeiters. Wenn der Mitarbeiter beispielsweise ein Update unmittelbar nach Erscheinen installiert, welches zu Inkompatibilitäten mit den institutionellen Anwendungen führt, kann dies zu einem Problem hinsichtlich der Verfügbarkeit führen. Vereinzelt sind Updates auch generell fehlerhaft und werden kurz nach dem Erscheinen wieder zurückgenommen. Eine IT-Administration wartet deshalb vor der Installation eines Updates in der Produktionsumgebung ggf. noch bzw. testet dieses vorab in einer Simulationsumgebung. Anders herum kann es aber auch problematisch sein, wenn der Mitarbeiter, etwa wegen der Inkompatibilität mit vorhandener Software, auf neue Updates verzichtet.

2.8 Automatisierte Synchronisation mit ungeeigneten Cloud-Diensten

Die umfangreicheren Rechte, die ein BYOD-Mitarbeiter auf seinem Gerät hat, geben ihm auch die Möglichkeit, Informationen mit externen Cloud-Diensten zu synchronisieren. Standardmäßig besteht dabei die Gefahr, dass dies auch institutionelle Informationen betreffen könnte und die Institution die Kontrolle darüber verliert, wo ihre Informationen gespeichert werden.

2.9 Ungeregelte Aussonderung von BYO-Geräten

Eine ungeregelte Aussonderung eines BYO-Geräts, bei dem etwa durch einen Defekt keine Löschung (Corporate-Wipe) mehr möglich war, stellt gegebenenfalls eine Gefahr für noch auf dem Gerät gespeicherte institutionelle Informationen dar.

2.10 Nicht oder unzureichend an BYOD angepasster Support

Die Möglichkeit zum zeit- und ortsunabhängigen Arbeiten mit BYOD stellt neue Herausforderungen an den Support der Institution. Es reicht ggf. nicht mehr aus einen Helpdesk während der Arbeitszeiten anzubieten, da BYOD-Mitarbeiter unter Umständen auch zu anderen Zeiten ein akutes Problem haben können, welches bei falscher Handhabung auch institutionelle Informationen gefährden kann.

2.11 Nutzung von BYO-Geräten durch Dritte

Haben Familienangehörige oder Freunde Zugang zum BYO-Gerät, können durch unsachgemäße Benutzung des Gerätes die institutionellen Informationen gefährdet werden.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.bd.8 *BYOD* aufgeführt. Grundsätzlich ist der Bausteinverantwortliche für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und regelmäßig überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter (ISB)

Weitere Verantwortliche	Administrator, Benutzer, Datenschutzbeauftragter, Institutionsleitung, IT-Betrieb, Leiter IT, Leiter Organisation, Personalabteilung, Personalrat/Betriebsrat, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein CON.bd.8 *BYOD* vorrangig umgesetzt werden:

CON.bd.8.A1 Konzept für BYOD [Datenschutzbeauftragter, Institutionsleitung, Personalabteilung, Personalrat/Betriebsrat]

Gemäß dem Risikoappetit der Institution MUSS diese im Vorfeld festlegen, in welcher Form der Einsatz von BYOD für die Institution sinnvoll und akzeptabel ist. Dazu MÜSSEN die betroffenen Geschäftsprozesse, Programme und Daten der Institution analysiert und daraufhin bewertet werden, ob diese für BYOD zur Verfügung stehen sollten. Der tatsächliche Bedarf sowie die entstehenden Kosten MÜSSEN dabei ergänzend in Betracht gezogen werden. Zusätzlich MUSS sichergestellt werden, dass die benötigten Ressourcen in personeller und technischer Hinsicht vorhanden sind bzw. hergestellt werden. Weiter MUSS bereits an dieser Stelle die Strategie bzgl. der unterstützten Endgeräte und ggf. deren Einschränkungen festgelegt werden.

CON.bd.8.A2 Regelungen für BYOD [Datenschutzbeauftragter, Institutionsleitung, Personalabteilung, Personalrat/Betriebsrat]

Die Institution MUSS ihren Mitarbeitern vorschreiben, wie BYOD stattfinden darf. Die Vereinbarung MUSS in Form einer Benutzerrichtlinie vor Freischaltung eindeutig akzeptiert werden. Mindestens muss darin geregelt werden:

- wer BYOD nutzen kann
- welche Voraussetzungen das Endgerät erfüllen
- das der Einsatz modifizierter Software grundsätzlich zu unterlassen ist
- in welchem Umfang BYOD eingesetzt werden kann
- unter welchen Bedingungen schützenswerte Informationen verarbeitet werden dürfen
- in welchem Umfang die Institution Zugriff auf das Gerät benötigt
- wie die privaten Informationen des Nutzers geschützt werden
- wie im Falle von Problemen Support geleistet wird
- welche Maßnahmen bei Verlust oder Diebstahl vorzunehmen sind
- wie sich die Nutzung von BYOD auf die Arbeitszeit auswirkt

CON.bd.8.A3 Absicherung des Gerätes vor fremdem Zugriff [Benutzer]

Zur Absicherung des Gerätes MUSS ein Zugriffscode, -passwort oder eine vergleichbare Absicherung (Fingerabdruck, Gesichtsscanner etc.) gesetzt und aktiviert werden. Die Passwörter MÜSSEN der Passwort-Richtlinie der Institution entsprechen, siehe ORP.4 *Identitäts- und Berechtigungsmanagement*.

CON.bd.8.A4 Nutzung einer abgesicherten Kommunikationsverbindung zur Institution [Benutzer]

Die Nutzung der Datendienste zur Institution MUSS über eine abgesicherte Kommunikationsverbindung nach Stand der Technik erfolgen.

CON.bd.8.A5 Bereitstellung einer Liste unterstützter Plattformen und Softwareversionen [IT-Betrieb]

Damit Mitarbeiter sicher sein können, passende Geräte für BYOD anzuschaffen, MUSS eine verbindliche Aufstellung kompatibler Plattformen und (Mindest-)Softwareversionen zur Verfügung gestellt und

regelmäßig aktualisiert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein CON.bd.8 *BYOD*. Sie SOLLTEN grundsätzlich umgesetzt werden.

CON.bd.8.A6 Nutzung einer Software zum Gerätemanagement [Leiter IT, IT-Betrieb]

Zur besseren zentralisierten Verwaltung SOLLTE eine Software zum Gerätemanagement (MDM) eingesetzt werden. Werden institutionelle Informationen auf dem Gerät verarbeitet, SOLLTE zudem zur Trennung von den privaten Aktivitäten der Einsatz einer Management-Software mit Container-Lösung (MAM, EMM, UEM) geprüft werden. Die Auswahl der passenden Lösung SOLLTE anhand des geplanten Funktionsumfanges erfolgen.

CON.bd.8.A7 Aktivierung automatischer Updates [Benutzer]

Damit immer die aktuellste Version des Betriebssystem genutzt wird, SOLLTE auf dem Endgerät die automatische Installation von Updates aktiviert und die Installation zeitnah vorgenommen werden.

CON.bd.8.A8 Schulungen für BYOD [Personalabteilung, Vorgesetzte]

Um die Mitarbeiter für die BYOD-Nutzung und die damit verbundenen Gefährdungen zu sensibilisieren, SOLLTEN in Regelmäßigkeit Schulungen zu den relevanten Themen (Awareness) freiwillig oder verpflichtend angeboten werden.

CON.bd.8.A9 Einschränkung der Nutzung von Software [Leiter IT, IT-Betrieb, Personalrat/Betriebsrat]

Zum Schutz der institutionellen Informationen vor ungeeigneter Verarbeitung SOLLTE der Einsatz einer Ausschluss- bzw. Freigabeliste (Black-/Whitelist) für Software geprüft werden. Diese SOLLTE als Bestandteil der Benutzerrichtlinie realisiert werden.

CON.bd.8.A10 Aktivierung von Funktionen zur entfernten Verwaltung [Benutzer]

Zur Absicherung gegen Verlust und Diebstahl SOLLTEN Funktionen zur Sperrung und Löschung aus der Ferne aktiviert werden. Falls diese nicht über Gerätedienste zur Verfügung stehen, SOLLTEN entsprechende Zusatzdienste dafür genutzt werden. Zur Vereinfachung der Verwaltung SOLLTE auf eine Möglichkeit zur zentralen Verwaltung geachtet werden.

CON.bd.8.A11 Aktivierung von Funktionen zur Absicherung [Benutzer]

Der Mitarbeiter SOLLTE verpflichtet werden, gerätespezifisch Hilfsprogramme wie ein Antivirus-Programm und eine Firewall zu installieren und auf dem aktuellen Stand zu halten. Zusätzlich SOLLTE ein sicherer Systemstart etwa durch Aktivierung des UEFI-SecureBoot (auf Notebooks) sichergestellt werden.

CON.bd.8.A12 Aktivierung von Funktionen zur Verschlüsselung [Benutzer]

Um die auf dem Gerät lokal gespeicherten Daten bestmöglich zu schützen, SOLLTEN Dienste zur Echtzeit-Verschlüsselung der Daten (BitLocker, FileVault etc.) aktiviert werden. Die Auswahl SOLLTE unter Berücksichtigung von CON.1 *Kryptokonzept* erfolgen.

CON.bd.8.A13 Anpassung des Supports für BYOD-Nutzung [Leiter IT, IT-Betrieb]

BYOD-Mitarbeiter SOLLTEN eine Unterstützung bei der Umsetzung der Anforderungen und auftretenden Problemen erhalten. Dieses Vorhaben kann mit der Bereitstellung von Informationen zur Selbsthilfe für häufig gestellte Fragen (FAQ) und Problemen, die außerhalb der Arbeitszeiten auftreten, realisiert werden. Hierfür SOLLTE geprüft werden, ob ergänzend eine Aufnahme in den üblichen Support der Institution vorgenommen werden kann.

CON.bd.8.A14 Bereitstellung eines Teilnetzes innerhalb der Institution für BYOD [Leiter IT, IT-Betrieb]

Damit BYO-Geräte nur Zugriff auf die vorgesehenen Ressourcen erhalten, SOLLTE im Netzwerk der Institution explizit ein Teilnetz für diese Geräte eingerichtet werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein CON.bd.8 *BYOD* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.bd.8.A15 Steuerung von Software-Aktualisierungen [Leiter IT, IT-Betrieb] (C,I)

Zur Vermeidung von Inkompatibilitäten SOLLTE die Administration darüber entscheiden wann Software-Aktualisierungen aufgespielt werden.

CON.bd.8.A16 Nutzung eindeutiger Identifizierung zum Zugriffsschutz [Leiter IT, IT-Betrieb] (C,I)

Zur Verbesserung der Sicherheit SOLLTE eine eindeutige Identifizierung und Freigabe von Diensten, etwa durch Zuhilfenahme der MAC-Adresse oder durch Nutzung von Fingerprinting des BYO-Geräts erfolgen.

CON.bd.8.A17 Nutzung von Zwei-Faktor-Authentifizierung [Benutzer] (C,I)

Zur Verbesserung der Sicherheit für schützenswerte Vorgänge SOLLTE, zusätzlich zum Zugriffscode, eine Zwei-Faktor-Authentifizierung eingesetzt werden.

4 Weiterführende Informationen

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein CON.bd.8 *BYOD* finden sich unter anderem in folgenden Veröffentlichungen:

[BSI2013]	Überblickspapier IT-Consumerisation und BYOD, BSI, Juli 2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 28.04.2019

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein CON.bd.8 *BYOD* von Bedeutung:

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.42 Social Engineering

G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

Elementare Gefährdungen Anforderungen	G 0.14	G 0.15	G 0.16	G 0.17	G 0.18	G 0.19	G 0.20	G 0.21	G 0.26	G 0.27	G 0.36	G 0.37	G 0.38	G 0.42	G 0.47
CON.bd.8.A1	X	X			X	X				X			X		X
CON.bd.8.A2	X	X	X	X	X	X	X				X	X	X		
CON.bd.8.A3	X		X	X							X	X	X		X
CON.bd.8.A4	X	X				X									X
CON.bd.8.A5					X		X			X					X
CON.bd.8.A6	X	X	X	X	X	X	X	X	X	X			X		
CON.bd.8.A7					X		X		X						X
CON.bd.8.A8	X	X	X	X	X	X	X	X	X		X		X	X	
CON.bd.8.A9		X			X		X		X	X			X		X
CON.bd.8.A10			X	X		X									
CON.bd.8.A11	X	X				X	X	X	X						X
CON.bd.8.A12	X		X	X		X									X
CON.bd.8.A13					X			X	X	X				X	
CON.bd.8.A14	X	X				X	X	X			X				X
CON.bd.8.A15					X		X		X						X
CON.bd.8.A16						X					X	X		X	
CON.bd.8.A17	X	X	X	X		X					X	X		X	